

Docket Content Report

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0001	Published Rule	Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items	5/20/2015	0
BIS-2015-0011-0084	BIS supplemental info	Intrusion and Surveillance Items FAQs 1-32 July 13 2015	7/13/2015	0
BIS-2015-0011-0002	Matthew Fisch	Kinetic Platforms Inc	5/20/2015	1
BIS-2015-0011-0003	Paul Pliska	Comment on FR Doc # 2015-11642	5/20/2015	0
BIS-2015-0011-0004	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/20/2015	0
BIS-2015-0011-0005	Chev Young	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0006	Eric Rand	Comment on FR Doc # 2015-11642	5/20/2015	0
BIS-2015-0011-0007	Every One	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0008	Chris Houser	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0009	James Pittman	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0010	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0011	Randy Wyatt	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0012	Jack Beglinger	Comment on FR Doc # 2015-11642	5/21/2015	0
BIS-2015-0011-0013	Anonymous	Comment on FR Doc # 2015-11642	5/22/2015	0
BIS-2015-0011-0014	PAWEL KRAWCZYK	Comment on FR Doc # 2015-11642	5/22/2015	0
BIS-2015-0011-0015	Jesse Friedman	Comment on FR Doc # 2015-11642	5/22/2015	0
BIS-2015-0011-0016	Michael Ober	Comment on FR Doc # 2015-11642	5/23/2015	0
BIS-2015-0011-0017	K Foster	Comment on FR Doc # 2015-11642	5/24/2015	0
BIS-2015-0011-0018	Matthew Bergin	Comment on FR Doc # 2015-11642	5/24/2015	0
BIS-2015-0011-0019	Jon Lvy	Comment on FR Doc # 2015-11642	5/25/2015	0
BIS-2015-0011-0020	Jacob Williams	Comment on FR Doc # 2015-11642	5/25/2015	0
BIS-2015-0011-0021	Scott Blaydes	Comment on FR Doc # 2015-11642	5/25/2015	0
BIS-2015-0011-0022	Clark Anonymous	Comment on FR Doc # 2015-11642	5/25/2015	0
BIS-2015-0011-0023	Willard Dawson	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0024	Jonathan Zdziarski	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0025	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0026	Anonymous Your boss	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0027	Charlie Miller	Comment on FR Doc # 2015-11642	5/26/2015	0

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0028	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0029	Bryan Owen	Comment on FR Doc # 2015-11642	5/26/2015	1
BIS-2015-0011-0030	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0031	leo gomez	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0032	Jasper Rogers	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0033	Gregory Hetrick	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0034	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0035	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0036	Tyler Nighswander	Comment on FR Doc # 2015-11642	5/26/2015	1
BIS-2015-0011-0037	Lucas Elmer	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0038	Rory McDonald	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0039	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0040	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/26/2015	0
BIS-2015-0011-0041	Jake Anonymous	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0042	John Labelle	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0043	Kerem Ylmaz	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0044	Luca C	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0045	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0046	Logan Browne	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0047	Joseph Leavitt	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0048	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0049	B. Calvin Saul	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0050	Joseph Autry	Comment on FR Doc # 2015-11642	5/27/2015	0
BIS-2015-0011-0051	Karim HadjSalem	Comment on FR Doc # 2015-11642	5/28/2015	0
BIS-2015-0011-0052	Matt Linton	Comment on FR Doc # 2015-11642	5/28/2015	0
BIS-2015-0011-0053	Stephen Marney	Comment on FR Doc # 2015-11642	5/28/2015	0
BIS-2015-0011-0054	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/29/2015	0
BIS-2015-0011-0055	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/29/2015	0
BIS-2015-0011-0056	Alex Green	Comment on FR Doc # 2015-11642	5/29/2015	0
BIS-2015-0011-0057	Anonymous Anonymous	Comment on FR Doc # 2015-11642	5/30/2015	0
BIS-2015-0011-0058	Rick Howard	Comment on FR Doc # 2015-11642	6/7/2015	0

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0059	Jason Syversen	Comment on FR Doc # 2015-11642	6/9/2015	0
BIS-2015-0011-0060	John Berry	Comment on FR Doc # 2015-11642	6/11/2015	0
BIS-2015-0011-0061	John Bryk	Comment on FR Doc # 2015-11642	6/11/2015	0
BIS-2015-0011-0062	Avindra Goolcharan	Comment on FR Doc # 2015-11642	6/15/2015	0
BIS-2015-0011-0063	Gregory Conti	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0064	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0065	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0066	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0067	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0068	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0069	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0070	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0071	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0072	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0073	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0074	Mike Frantzen	Comment on FR Doc # 2015-11642	6/17/2015	0
BIS-2015-0011-0076	Richard Farina	Comment on FR Doc # 2015-11642	7/6/2015	0
BIS-2015-0011-0077	Anonymous Anonymous	Comment on FR Doc # 2015-11642	6/29/2015	0
BIS-2015-0011-0078	Andrew Sullivan	Comment on FR Doc # 2015-11642	6/24/2015	0
BIS-2015-0011-0079	Richard McCutcheon	Comment on FR Doc # 2015-11642	6/20/2015	0
BIS-2015-0011-0080	Rachel Marsden	Comment on FR Doc # 2015-11642	6/20/2015	1
BIS-2015-0011-0081	Andrew Auernheimer	Comment on FR Doc # 2015-11642	6/19/2015	1
BIS-2015-0011-0082	Howard Ehrlich	Fidelis Cybersecurity	6/19/2015	1
BIS-2015-0011-0083	Richard Farina	Comment on FR Doc # 2015-11642	7/6/2015	0
BIS-2015-0011-0085	James Gannon	Cyber Invasion LCD	7/11/2015	1
BIS-2015-0011-0086	Paul Pliska	Comment on FR Doc # 2015-11642	7/15/2015	0
BIS-2015-0011-0087	Dale Adams	Comment on FR Doc # 2015-11642	7/15/2015	0
BIS-2015-0011-0088	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/16/2015	0
BIS-2015-0011-0089	Nicholas Weaver	Comment on FR Doc # 2015-11642	7/16/2015	0
BIS-2015-0011-0090	Kevin Schoonmaker	Comment on FR Doc # 2015-11642	7/16/2015	0
BIS-2015-0011-0091	Rolf Rolles	Comment on FR Doc # 2015-11642	7/16/2015	0
BIS-2015-0011-0092	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/16/2015	0

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0093	Albert Walton	Comment on FR Doc # 2015-11642	7/16/2015	0
BIS-2015-0011-0094	Shad Nygren	Comment on FR Doc # 2015-11642	7/17/2015	0
BIS-2015-0011-0095	Cody Curtis	Comment on FR Doc # 2015-11642	7/17/2015	0
BIS-2015-0011-0096	Alan Amesbury	Comment on FR Doc # 2015-11642	7/17/2015	0
BIS-2015-0011-0097	William Root	Comment on FR Doc # 2015-11642	6/14/2015	1
BIS-2015-0011-0098	Watson Ladd	Comment on FR Doc # 2015-11642	5/20/2015	1
BIS-2015-0011-0099	Scott Francis	Comment on FR Doc # 2015-11642	5/20/2015	1
BIS-2015-0011-0100	Richard Bradley	Comment on FR Doc # 2015-11642	5/22/2015	1
BIS-2015-0011-0101	Julia Court Ryan & Karl Abendschein	Raytheon BIS Cybersecurity Rule - Extension Request	7/10/2015	1
BIS-2015-0011-0102	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/17/2015	0
BIS-2015-0011-0103	Justin Yakoski	Comment on FR Doc # 2015-11642	6/16/2015	1
BIS-2015-0011-0104	David Wilburn	Comment on FR Doc # 2015-11642	7/16/2015	1
BIS-2015-0011-0105	Christopher Carlson	Comment on FR Doc # 2015-11642	7/17/2015	0
BIS-2015-0011-0106	Martin Peck	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0107	Richard Salz	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0108	Matthew Goldstein	GPLLC	7/19/2015	1
BIS-2015-0011-0109	Nicholas Kain	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0110	Kevin O'Connor	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0111	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0112	Ozan Munsuz	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0113	Andrew Pietila	Comment on FR Doc # 2015-11642	7/19/2015	0
BIS-2015-0011-0114	Nate Lawson	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0115	Matthew Murphy	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0116	James Ford	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0117	Craig Nelson	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0118	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0119	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0120	Nicholas Weaver	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0121	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0122	Paul Nash	Comment on FR Doc # 2015-11642	7/20/2015	0

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0123	Jonathan Walker	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0124	Jonathan Janego	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0125	Michael VanZant	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0126	John Doe	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0127	Peter Hesse	10Pearls, LLC	7/20/2015	1
BIS-2015-0011-0128	Russel Van Tuyl	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0129	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0130	Matthew Joyce	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0131	Brian Scarpelli	TIA Comments	7/20/2015	1
BIS-2015-0011-0132	Todd Jarvis	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0133	Bas Alberts	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0134	Justin Malyn	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0135	Anonymous foreigner	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0136	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0137	Ingrid Skoog	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0138	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0139	Kevin Johnson	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0140	Jacob Osborn	Offensive Security	7/20/2015	1
BIS-2015-0011-0141	Raphael Mudge	Cobalt Strike	7/20/2015	1
BIS-2015-0011-0142	Jacob Osborn	Pwnie Express	7/20/2015	1
BIS-2015-0011-0143	Michael Beckerman	Internet Association	7/20/2015	1
BIS-2015-0011-0144	Jim Wojno	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0145	Cheri McGuire	Symantec	7/20/2015	1
BIS-2015-0011-0146	David Aitel	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0146	David Aitel	Immunity Inc	7/20/2015	2
BIS-2015-0011-0147	Jacob Ansari	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0148	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0149	Robert Radvanovsky	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0150	Jacob Osborn	Core Security	7/20/2015	1
BIS-2015-0011-0151	Anonymous Anonymous	Rapid7	7/20/2015	1

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0152	Allen Householder & Art Manion	CERT Carnegie Mellon University	7/20/2015	1
BIS-2015-0011-0153	Christian Troncoso	BSA The Software Alliance	7/20/2015	1
BIS-2015-0011-0154	Fred Powell	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0155	Ryan Corcoran	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0156	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0157	Ronnie Tokazowski	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0158	Garve Hays	Net IQ	7/20/2015	1
BIS-2015-0011-0158	Geoff Sanders	Launch Key	7/20/2015	2
BIS-2015-0011-0158	Morey Haber	Beyond Trust	7/20/2015	3
BIS-2015-0011-0158	Robert Hansen	White Hat	7/20/2015	4
BIS-2015-0011-0158	Ryan Smith	Accuvant	7/20/2015	5
BIS-2015-0011-0158	Tom Gorup	Rook Security	7/20/2015	6
BIS-2015-0011-0158	Tomer Schwartz	Adallom	7/20/2015	7
BIS-2015-0011-0159	Cristin Goodwin	Microsoft	7/20/2015	1
BIS-2015-0011-0160	Tom Cross	Drawbridge Networks	7/20/2015	1
BIS-2015-0011-0161	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0162	Sam Houston	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0163	Nathaniel Vos	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0164	Jacob Brodsky	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0165	Robert Graham'	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0166	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0167	Dave Weinstein	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0168	John Anderson	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0169	Dave Lewis	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0170	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0171	Adam Pridgen	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0172	Mara Tam	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0173	Amir Etemadieh	Exploiters	7/20/2015	1
BIS-2015-0011-0174	Joseph FitzPatrick	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0175	Christopher Eng	Comment on FR Doc # 2015-11642	7/20/2015	1

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0176	Michael Ossmann	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0177	Tony Webster	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0178	Adam Caudill	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0179	Karl Koscher	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0180	Travis Roesner	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0181	Billy Rios	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0182	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0183	Nick Galbreath	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0184	Marsh Ray	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0185	David Longenecker	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0186	Christopher Soghoian	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0187	Steve Roggenkamp	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0188	Sergey Bratus	Darthmouth College	7/20/2015	1
BIS-2015-0011-0189	Berin Szoka	TechFreedom	7/20/2015	1
BIS-2015-0011-0190	Anonymous Anonymous	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0191	Dan Kaminsky	White Ops	7/20/2015	1
BIS-2015-0011-0192	Frank Martinjak	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0193	Carl Mehner	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0194	Corey Thuen	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0195	Anton Schieffer	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0196	David Longenecker	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0197	Wayne Baisley	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0198	Ryan Castellucci	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0199	Jose Fernandez	CompSecDirect	7/20/2015	1
BIS-2015-0011-0200	Michael James	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0201	Dino Dai Zovi	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0202	Douglas Twitchell	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0203	Michael Toecker	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0204	Christina Wuest	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0205	Jesse Lyon	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0206	William Showalter	Comment on FR Doc # 2015-11642	7/20/2015	0
BIS-2015-0011-0207	Laurence K Disenhof	EDA Consortium (EDAC)	7/17/2015	1

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0208	Congressmen: Langevin, Schweikert, McCaul, Lieu	Congressional Wassenaar Comments	7/20/2015	1
BIS-2015-0011-0209	Meredith Rathbone	Steptoe & Johnson, on behalf of Coalition for Responsible Cybersecurity	7/20/2015	1
BIS-2015-0011-0210	Masahiro Uemura (Director), Takuma Maeda (Assistant Director)	SET Comments from Japanese private sector METI	7/20/2015	1
BIS-2015-0011-0211	Dean C. Garfield	Information Technology Industry Council (ITI)	7/20/2015	1
BIS-2015-0011-0212	Roszel C. Thomsen II	Alliance for Network Security Comments on WA 2013 Cyber Rule	7/20/2015	1
BIS-2015-0011-0213	Jeff Rittener	Intel Corporation Comments	7/20/2015	1
BIS-2015-0011-0214	Ken Montgomery	CompTIACommentsDOCWass2013ProposedRuleFinalClean	7/20/2015	1
BIS-2015-0011-0215	Cynthia Johnson & Mario R. Palacios	SIA Comments on Cybersecurity	7/20/2015	1
BIS-2015-0011-0216	Jonathan Brossard	Toucan System	7/22/2015	1
BIS-2015-0011-0217	Mike Ward	Technet	7/17/2015	1
BIS-2015-0011-0218	Amy Ross	Red Hat	7/20/2015	1
BIS-2015-0011-0219		Privacy International BIS submission	7/20/2015	1
BIS-2015-0011-0220	Ryan Gillis	Palo Alto Networks	7/20/2015	1
BIS-2015-0011-0221	Jim Ramsbotham	OEI Tech FINAL	7/20/2015	1
BIS-2015-0011-0222	Tom donovan	Northrop Grumman	7/20/2015	1
BIS-2015-0011-0223	Linda Dempsey	National Association of Manufactures (NAM)	7/20/2015	1
BIS-2015-0011-0224	Abigail Slater	Internet Association	7/20/2015	1
BIS-2015-0011-0225	Edward A Bond	IBM Cyber Rule Comments	7/20/2015	1
BIS-2015-0011-0226	Howard Grodin	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0227	Katie Moussouris	HackerOne	7/21/2015	1

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0228	Neil Martin	Google Comment	7/20/2015	1
BIS-2015-0011-0229	Frank McClain	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0230		FireEye Comments Wassenaar	7/20/2015	1
BIS-2015-0011-0231	Richard Foster	Financial Services Roundtable-BITS	7/20/2015	1
BIS-2015-0011-0232		Final Group Letter	7/20/2015	1
BIS-2015-0011-0233	Eric Wenger	Cisco	7/20/2015	1
BIS-2015-0011-0234	Jacob Torrey	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0235	Jeff Jarmoc	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0238	John Lampe	Tenable	7/20/2015	1
BIS-2015-0011-0239	Mario Santana	Risk Analytics	7/20/2015	1
BIS-2015-0011-0240	Keith Seymour	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0241	Kristian Erik Hermansen	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0242	Willis Vandevanter	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0243	Matt Weeks	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0244	Mike Clark	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0245	Dan Tentler	Carbon Dynamics Dan Tentler	7/20/2015	1
BIS-2015-0011-0246	Sandra Bittner	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0247	Aaron P Padilla	API cover memo	7/20/2015	1
BIS-2015-0011-0248	Thomas Dulien	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0249	Alan Saqui	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0250	Peter Ryan Jr.	Rochester Institute of Technology	7/20/2015	1
BIS-2015-0011-0251	Chris Sullo	Comment on FR Doc # 2015-11642	7/20/2015	1
BIS-2015-0011-0253	Michael Hunter	Comment on FR Doc # 2015-11642	7/21/2015	1
BIS-2015-0011-0254	West Coile	Comment on FR Doc # 2015-11642	7/21/2015	1
BIS-2015-0011-0255	David A Wheeler	Comment on FR Doc # 2015-11642	7/21/2015	1
BIS-2015-0011-0256	JD Postage	Comment on FR Doc # 2015-11642	7/21/2015	1
BIS-2015-0011-0257	Joshua Millan	ViaSat	7/20/2015	1
BIS-2015-0011-0258	Anthon V Jones	USTelecom	7/20/2015	1
BIS-2015-0011-0259	Kyle Hanslovan	StrategicIO	7/20/2015	1
BIS-2015-0011-0261	Nate Cardozo	Electronic Frontier Foundation	7/20/2015	1
BIS-2015-0011-0262	York Huang	Electric Power Research Institute	7/20/2015	1
BIS-2015-0011-0263	Nandkumar Saravade	Data Security Council of India (DSCI)	7/20/2015	1

Document ID	Submitter Name	Document Title	Received Date	Attachment Nbr
BIS-2015-0011-0264	Andy Slayer	Center for Technology Democracy	7/20/2015	1
BIS-2015-0011-0266	Christopher Haave	Boeing	7/20/2015	1
BIS-2015-0011-0267	Michael Angelo	Pre-rule review by TAC member	4/13/2015	1

and/or RIN in the subject line of the message. Submit electronic comments in Word Perfect, Microsoft Word, PDF, or ASCII file format, and avoid the use of special characters or any form on encryption.

3. *Postal Mail*: Ms. Brenda Edwards, U.S. Department of Energy, Building Technologies Office, Mailstop EE-5B, 1000 Independence Avenue SW., Washington, DC 20585-0121. If possible, please submit all items on a compact disc (CD), in which case it is not necessary to include printed copies.

4. *Hand Delivery/Courier*: Ms. Brenda Edwards, U.S. Department of Energy, Building Technologies Office, 950 L'Enfant Plaza SW., Suite 600, Washington, DC 20024. Telephone: (202) 586-2945. If possible, please submit all items on a CD, in which case it is not necessary to include printed copies.

No telefacsimilies (faxes) will be accepted. For detailed instructions on submitting comments and additional information on the rulemaking process, see the "Public Participation" section of the March 31, 2015 NOPR. 80 FR 17222.

Docket: The docket, which includes **Federal Register** notices, public meeting attendee lists and transcripts, comments, and other supporting documents/materials, is available for review at www.regulations.gov. All documents in the docket are listed in the www.regulations.gov index. However, not all documents listed in the index may be publically available, such as those containing information that is exempt from public disclosure.

A link to the docket Web page can be found at: <http://www.regulations.gov/#!docketDetail;D=EERE-2012-BT-STD-0047>. This Web page contains a link to the docket for this notice on the www.regulations.gov site. The www.regulations.gov Web page contains simple instructions on how to access all documents, including public comments, in the docket. See section VII, "Public Participation," of the March 31, 2015 NOPR for further information on how to submit comments through www.regulations.gov.

For further information on how to submit a comment or review other public comments and the docket, contact Ms. Brenda Edwards at (202) 586-2945 or by email: Brenda.Edwards@ee.doe.gov.

FOR FURTHER INFORMATION CONTACT: Mr. John Cymbalsky, U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy, Building Technologies Office, EE-5B, 1000 Independence Avenue SW., Washington, DC 20585-0121.

Telephone: (202) 287-1692. Email: residential_furnaces_and_boilers@ee.doe.gov.

Mr. Eric Stas, U.S. Department of Energy, Office of the General Counsel, GC-33, 1000 Independence Avenue SW., Washington, DC 20585-0121. Telephone: (202)-5869507. Email: Eric.Stas@hq.doe.gov.

For information on how to submit or review public comments and the docket, contact Ms. Brenda Edwards at (202) 586-2945 or by email: Brenda.Edwards@ee.doe.gov.

SUPPLEMENTARY INFORMATION: DOE published a NOPR in the **Federal Register** to make available and invite public comments on its analysis regarding potential energy conservation standards for residential boilers. 80 FR 17222 (March 31, 2015). The document set a deadline for the submission of written comments by June 1, 2015. The Air-Conditioning, Heating, and Refrigeration Institute (AHRI) and the Oil Heat Manufacturers Association each requested an extension of the public comment period, stating that additional time is necessary to review the published analysis in order to prepare and submit comments. After careful consideration of these requests, DOE has determined that extending the comment period to allow additional time for interested parties to submit comments is appropriate based on the foregoing reason. DOE believes that extending the comment period by 30 days will provide the public with sufficient time to submit comments responding to DOE's analysis. Accordingly, DOE is extending the comment period to midnight of July 1, 2015, and will deem any comments received (or postmarked) by that date to be timely submitted.

Issued in Washington, DC, on May 12, 2015.

Kathleen B. Hogan,

Deputy Assistant Secretary for Energy Efficiency and Renewable Energy.

[FR Doc. 2015-12219 Filed 5-19-15; 8:45 am]

BILLING CODE 6450-01-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Parts 740, 742, 748, 772, 774

[Docket No. 150304218-5218-01]

RIN 0694-AG49

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Proposed rule, with request for comments.

SUMMARY: The Bureau of Industry and Security (BIS) proposes to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013 with regard to systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor. BIS proposes a license requirement for the export, reexport, or transfer (in-country) of these cybersecurity items to all destinations, except Canada. Although these cybersecurity capabilities were not previously designated for export control, many of these items have been controlled for their "information security" functionality, including encryption and cryptanalysis. This rule thus continues applicable Encryption Items (EI) registration and review requirements, while setting forth proposed license review policies and special submission requirements to address the new cybersecurity controls, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items.

BIS also proposes to add the definition of "intrusion software" to the definition section of the EAR pursuant to the WA 2013 agreements.

DATES: Submit comments on or before July 20, 2015.

ADDRESSES: Comments on this rule may be submitted to the Federal rulemaking

portal (www.regulations.gov). The regulations.gov ID for this rule is: BIS-2015-0011. Comments may also be submitted via email to publiccomments@bis.doc.gov or on paper to Regulatory Policy Division, Bureau of Industry and Security, Room 2099B, U.S. Department of Commerce, 14th St. and Pennsylvania Ave. NW., Washington, DC 20230. Please refer to RIN 0694-AG49 in all comments and in the subject line of email comments.

FOR FURTHER INFORMATION CONTACT:

Catherine Wheeler, Director, Information Technology Control Division, Phone: (202) 482-0707 or by email at Catherine.Wheeler@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

The Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a group of 41 like-minded states committed to promoting responsibility and transparency in the global arms trade, and preventing destabilizing accumulations of arms. As a Participating State, the United States has committed to controlling for export all items on the WA control lists. The lists were first established in 1996 and have been revised annually thereafter. Proposals for changes to the WA control lists that achieve consensus are approved by Participating States at annual December Plenary meetings. Participating States are charged with implementing the agreed list changes as soon as possible after approval. Implementation of WA list changes ensures U.S. companies have a level playing field with their competitors in other WA member states.

In 2013, WA agreed to add the following to their list of dual-use goods: systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor. BIS, the Departments of Defense and State, as well as other agencies have been discussing the best way to add these

items, which we have named “cybersecurity items,” to the Commerce Control List (CCL) (Supplement No. 1 to part 774 of the Export Administration Regulations) without reducing encryption controls and while balancing the national security and foreign policy. For resource planning purposes, as well as license requirements, license exceptions, license submission requirements, and internal license reviews and processing planning purposes, this rule is published as a proposed rule.

Scope of the New Entries

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices. The new entry on the CCL that would control Internet Protocol (IP) network communications surveillance systems or equipment is restricted to products that perform all of the functions listed; however, the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry.

Addition of ECCNs 4A005 and 4D004 to the Commerce Control List

This rule proposes to add Export Control Classification Number (ECCN) 4A005 (“systems,” “equipment,” or “components” therefor, “specially designed” for the generation, operation or delivery of, or communication with, “intrusion software”) and ECCN 4D004 (“software” “specially designed” for the generation, operation or delivery of, or communication with, “intrusion software”) to the CCL. These ECCNs are proposed to be controlled for national security (NS), regional stability (RS), and anti-terrorism (AT) reasons to all destinations, except Canada. No license exceptions would be available for these items, except certain provisions of License Exception GOV, e.g., exports to or on behalf of the United States Government pursuant to § 740.11(b) of the EAR. This rule also proposes adding a License Requirement Note and a Note in the Related Controls paragraph for

these ECCNs, to alert exporters to include all relevant information when submitting classification requests and licensing applications.

ECCN 4D001

This rule also proposes to amend ECCN 4D001 by adding ECCN 4A005 to Items paragraph 4D001.a in order to add control of “software” “specially designed” or modified for the “development” or “production,” of equipment controlled by 4A005; adding an RS:1 license requirement paragraph for 4D001.a (as it applies to 4A005 or 4D004), removing License Exceptions TSR and STA eligibility; and adding the same explanatory License Requirement Note and Related Controls Note that would be added to ECCNs 4A005 and 4D004.

As a technical correction, this rule proposes to remove from the “Reason for control” paragraph “NP,” and from the License Requirement section the two sentences, “NP applies, unless a license exception is available. See § 742.3(b) of the EAR for information on applicable licensing review policies.” That text does not articulate any license requirement, and no nuclear non-proliferation license requirement for software classified as 4D001 is set forth elsewhere in the EAR. BIS’s regular practice is to impose a license requirement for nuclear non-proliferation reasons on items that are specified on the “List of Nuclear-Related Dual-Use Equipment, Materials, Software, and Related Technology” by the Nuclear Suppliers Group. ECCN 4D001 software is not so specified.

ECCN 4E001

This rule also proposes to amend ECCN 4E001 by adding a new Items paragraph 4E001.c to control “technology” “required” for the “development” of “intrusion software.” ECCN 4E001.a controls ““technology” according to the General Technology Note, for the “development,” “production,” or “use” of equipment or “software” controlled by 4A (except 4A980 or 4A994) or 4D (except 4D980, 4D993 or 4D994).” Therefore, ECCN 4E001.a would control “technology” for the newly added 4A005 and 4D004, as well as 4D001.a (for 4A005 and 4D004). This rule also proposes to add an RS:1 license requirement paragraph for 4E001.a “technology” (as it applies to 4A005, 4D001.a (as it applies to 4A005 or 4D004) and 4E001.c, which would require a license to export, reexport, and transfer (in-country) to all destinations, except Canada. BIS also proposes to remove License Exception Technology and Software Under

Restriction (TSR) and Strategic Trade Authorization (STA) eligibility and add the same explanatory License Requirement Note and Related Controls Note added to ECCNs 4A005, 4D001 and 4D004. Also, a reference to § 772.1 is proposed to be added to ECCNs 4A005, 4D001 and 4E001 to point to the location of the “intrusion software” definition, as this rule may be of interest to many new exporters that would not otherwise know that double quoted terms in the EAR are defined in § 772.1.

Lastly, the same technical correction regarding the Nuclear Non-proliferation (NP) control is proposed for 4E001 as is proposed for 4D001, see explanation above.

ECCN 5A001.j: Internet Protocol (IP) Network Communications Surveillance Systems or Equipment and Test, Inspection, Production Equipment, Specially Designed Components Therefor

Network communication traffic analysis systems are becoming an increasingly sensitive issue, which is why WA agreed to add the control of these items to the WA dual-use list. These systems are using the process of intercepting and analyzing messages to produce personal, human and social information from the communications traffic. BIS proposes to add these items in paragraph 5A001.j and group them with cybersecurity items. The license requirements for these items are proposed to under NS Column 1, RS Column 1 and AT Column 1 on the Commerce Country Chart (Supplement No. 1 to part 738 of the EAR) and would require a license for export, reexport, and transfer (in-country) to all destinations, except Canada. Only certain provisions of License Exception GOV, *e.g.*, exports to or on behalf of the United States Government pursuant to § 740.11(b) of the EAR, would be available for these items.

The same addition of a License Requirement Note and Related Control Note is proposed for ECCNs 5A001, 5D001, and 5E001 as is proposed for ECCNs 4A005, 4D001, 4D004 and 4E001 (see explanation under 4A005 and 4D005 above).

§ 740.13—License Exception TSU

BIS proposes to remove cybersecurity software from the mass market provision of License Exception TSU eligibility by adding a new paragraph (d)(2)(ii). This is consistent with the existing encryption exclusion.

Cybersecurity Items That Are Designed or Modified To Use “Cryptography” or Cryptanalysis

As previously introduced and explained in the preamble, this rule proposes to add a Related Control note to ECCNs 4A005, 4D004, 4E001, 5A001, 5A002, 5D002 and 5E002 that states that cybersecurity items are classified in cybersecurity ECCNs, even if the items are designed or modified to use “cryptography” or cryptanalysis; however, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD. This note is added so that people will not be confused under which ECCN to classify their products and when a cybersecurity item is designed or modified to use “cryptography” or cryptanalysis, after the relevant Encryption Items (EI) requirements for registration and review have been separately satisfied. One effect this will have is that these cybersecurity items will not be eligible for License Exception ENC. However, BIS anticipates licensing broad authorizations to certain types of end users and destinations that will counterbalance the loss of the use of License Exception ENC.

Information To Be Submitted With a License Application To Export, Reexport, or Transfer (In-Country) Cybersecurity Items

In addition to the general information required by § 748.3(b) of the EAR and the requirement that all encryption registration and review provisions must be separately satisfied with BIS and the ENC Encryption Request Coordinator, Ft. Meade, MD, this rule proposes to add a requirement to submit specific technical information in support of applications to export, reexport, or transfer (in-country) cybersecurity items. The specified technical information is set forth in newly added paragraph (z) of Supplement No. 2 to part 748 “Unique application and submission requirements.” The Commodity Classification Application Tracking System (CCATS) number(s) or license number(s) for the cyber security item(s) must be included in the license application. If no classification or license application has been done for the cybersecurity item, then the answers

to three (3) questions are to be submitted in a letter of explanation.

Also, this rule proposes that upon request from BIS, the applicant must include a copy of the sections of source code and other software (*e.g.*, libraries and header files) that implement or invoke the controlled cybersecurity functionality.

License Review Policy for Cybersecurity Items

The license review policies for cybersecurity items controlled under NS and AT will not be revised. A new license review policy for cybersecurity items is proposed under § 742.6(b) for regional stability. Cybersecurity items controlled for RS are proposed to be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, foreign commercial partners located in Country Group A:5, government end users in Australia, Canada, New Zealand or the United Kingdom, and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including the foreign policy interest of promoting the observance of human rights throughout the world. Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities. The governments of Australia, Canada, New Zealand or the United Kingdom have partnered with the United States on cybersecurity policy and issues, which affords these countries with favorable treatment for license applications. A note that describes “foreign commercial partner” is proposed to be added to § 742.6(b). Any “information security” functionality incorporated in the cybersecurity item will also receive a focused case-by-case review for reasons of Encryption Items (EI) control.

§ 772.1 Definitions of Terms as Used in the EAR: Addition of Definition for “Intrusion Software”

The WA-agreed definition for “intrusion software” is proposed to be added to § 772.1 of the EAR. The definition also includes a Note that describes some items not included as “intrusion software,” *e.g.*, hypervisors, debuggers or Software Reverse Engineering (SRE).

Request for Comments

BIS is seeking information about the effect of this rule and would appreciate the submission of comments, and especially answers to the following questions:

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

a. How many additional applications would be for products that are currently eligible for license exceptions?

b. How many additional applications would be for products that currently are classified EAR99?

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

* The **ADDRESSES** section of this proposed rule includes information about how to submit comments.

Rulemaking Requirements

1. Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This rule has been designated a "significant regulatory action," under Executive Order 12866.

2. Notwithstanding any other provision of law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection of information subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA), unless that collection of information displays a currently valid Office of Management and Budget (OMB) Control Number. This rule would involve one collection of information subject to the PRA. One of the collections has been approved by OMB under control number 0694-0088, "Multi-Purpose Application," and carries a burden hour estimate of 58 minutes for a manual or electronic submission. The additional information proposed to be required under

Supplement No. 2 to part 748 paragraph (z) falls under the usual technical information that is submitted with applications to describe the abilities of the items on the license application.

This information allows the licensing officer to verify the classification of the product and determine the effect it would have on U.S. national security and foreign policy. Send comments regarding these burden estimates or any other aspect of these collections of information, including suggestions for reducing the burden, to OMB Desk Officer, New Executive Office Building, Washington, DC 20503; and to Jasmeet Seehra, OMB Desk Officer, by email at Jasmeet_K_Seehra@omb.eop.gov or by fax to (202) 395-7285; and to the Office of Administration, Bureau of Industry and Security, Department of Commerce, 1401 Constitution Ave. NW., Room 6622, Washington, DC 20230.

3. This rule does not contain policies with Federalism implications as that term is defined under Executive Order 13132.

4. The provisions of the Administrative Procedure Act (APA) (5 U.S.C. 553) requiring notice of proposed rulemaking, the opportunity for public participation, and a 30-day delay in effective date, are inapplicable because this regulation involves a military and foreign affairs function of the United States (5 U.S.C. 553(a)(1)). Nonetheless, BIS is providing the public with an opportunity to review and comment on this rule, despite its being exempted from that requirement of the APA. Because this rule is not required by the APA to undergo a period of notice and comment, the requirements of the Regulatory Flexibility Act, 5 U.S.C. 601 *et seq.*, do not apply. Accordingly, no regulatory flexibility analysis is required, and none has been prepared.

BIS is interested in the potential impacts to businesses of this rule. Because most of the items impacted by this rule have encryption capabilities, BIS believes they are already being controlled under Category 5 part 2 of the EAR. Even though most encryption items are eligible for License Exception ENC and these cybersecurity items will not be eligible for License Exception ENC, BIS anticipates issuing broad licenses for these items. The impact of this rule is unknown to BIS, therefore the implementation of the Wassenaar Arrangement agreement of 2013 with regard to cybersecurity items is issued as a proposed rule with request for comments concerning the impact of the rule. Comments should be submitted to Sharron Cook, Office of Exporter Services, Bureau of Industry and Security, Department of Commerce,

14th and Pennsylvania Ave. NW., Room 2099, Washington, DC 20230 or emailed to publiccomments@bis.doc.gov. Please refer to RIN 0694-AG49 in all comments and in the subject line of email comments.

List of Subjects

15 CFR Part 740

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 742

Exports, Terrorism.

15 CFR Part 748

Administrative practice and procedure, Exports, Reporting and recordkeeping requirements.

15 CFR Part 772

Exports.

15 CFR Part 774

Exports, Reporting and recordkeeping requirements.

Accordingly, parts 740, 742, 748, 772, and 774 of the Export Administration Regulations (15 CFR parts 730 through 774) are proposed to be amended as follows:

PART 740 [AMENDED]

■ 1. The authority citation for part 740 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 7201 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

■ 2. Section 740.2 is amended by adding paragraph (a)(19) to read as follows:

§ 740.2 Restrictions on all License Exceptions.

(a) * * *

(19) The item is a cybersecurity item, *i.e.*, those controlled by ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" for 5A001.j items), 5D001.c ("specially designed" for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a (for 5A001.j items) or 5D001.c ("specially designed" for 5A001.j or 5B001.a items) and the export, reexport or transfer (in-country) is not authorized by § 740.11(b)(2)(ii) (made by or consigned to a department or agency of the U.S. government), or

§ 740.11(b)(2)(iii) (made for or on behalf of a department or agency of the U.S. Government).

* * * * *

- 3. Section 740.11 is amended by:
 - a. Adding paragraph (a)(2)(vi);
 - b. Removing the “or” from the end of paragraph (c)(3)(vi);
 - c. Removing the period from paragraph (c)(3)(vii) and adding a semicolon in its place; and
 - d. Adding paragraph (c)(3)(viii).

The revisions and addition read as follows:

§ 740.11 Governments, international organizations, international inspections under the Chemical Weapons Convention, and the International Space Station (GOV).

- (a) * * *
- (2) * * *

(vi) Cybersecurity items, *i.e.*, those controlled by ECCNs 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items), 4D004, 4E001.a (“required” for 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a (“specially designed” for 5A001.j items), 5D001.a (“specially designed” or modified for 5A001.j items), 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) or 5E001.a (“required” for 5A001.j, 5B001.a, 5D001.a (“specially designed” or modified for 5A001.j items) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items).

- * * * * *
- (c) * * *
- (3) * * *

(viii) Cybersecurity items, *i.e.*, those controlled by ECCNs 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items), 4D004, 4E001.a (“required” for 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j, 5B001.a (“specially designed” for 5A001.j items), 5D001.a (“specially designed” or modified for 5A001.j items), 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) or 5E001.a (“required” for 5A001.j, 5B001.a, 5D001.a (“specially designed” or modified for 5A001.j items) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items).

* * * * *

- 4. Section 740.13 is amended by revising the section heading and paragraph (d)(2) to read as follows:

§ 740.13 Technology and Software—Unrestricted (TSU).

- * * * * *
- (d) * * *

(2) *Exclusions*—(i) *Encryption software*. The provisions of this paragraph (d) are not available for encryption software controlled for “EI” reasons under ECCN 5D002 or for encryption software with symmetric key length exceeding 64-bits that qualifies as mass market encryption software under the criteria in the Cryptography Note (Note 3) of Category 5, Part 2, of the Commerce Control List (Supplement No. 1 to part 774 of the EAR). (Once such mass market encryption software has been reviewed by BIS and released from “EI” and “NS” controls pursuant to § 742.15(b) of the EAR, it is controlled under ECCN 5D992.c and is thus outside the scope of License Exception TSU.) See § 742.15(b) of the EAR for exports and reexports of mass market encryption products controlled under ECCN 5D992.c.

(ii) *Cybersecurity software*. The provisions of this paragraph (d) are not available for cybersecurity “software” that is classified under ECCNs 4D001.a (“specially designed” or modified for 4A005 or 4D004 items), 4D004, or for “software” under ECCN 5D001.a or .c (“specially designed” for “production,” “development” or “use” of 5A001.j equipment or systems, or providing the characteristics, functions or features of 5A001.j or 5B001.a equipment or systems).

* * * * *

- 5. Section 740.17 is amended by revising paragraph (b)(3)(iii) introductory text to read as follows:

§ 740.17 Encryption commodities, software and technology (ENC).

- * * * * *
- (b) * * *
- (3) * * *

(iii) Encryption commodities and software not described by paragraph (b)(2) of this section, and not further controlled for NS and RS reasons under ECCNs 5A001.j, 5B001.a (“specially designed” for 5A001.j), 5D001.a (“specially designed” or modified for 5A001.j) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a), that provide or perform vulnerability analysis, network forensics, or computer forensics functions characterized by any of the following:

* * * * *

- 6. Section 740.20 is amended by adding paragraph (b)(2)(ix) to read as follows:

§ 740.20 License Exception Strategic Trade Authorization (STA).

- * * * * *
- (b) * * *
- (2) * * *

(ix) License Exception STA may not be used for any cybersecurity items, *i.e.*, those controlled by ECCNs 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items), 4D004, 4E001.a (“required” for 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items) or 4D004 items), 4E001.c, 5A001.j, 5B001.a (“specially designed” for 5A001.j items), 5D001.a (“specially designed” or modified for 5A001.j items), 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) or 5E001.a (“required” for 5A001.j, 5B001.a, 5D001.a (“specially designed” or modified for 5A001.j items) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) items).

* * * * *

PART 742 [AMENDED]

- 7. The authority citation for part 742 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 22 U.S.C. 3201 *et seq.*; 42 U.S.C. 2139a; 22 U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; Sec. 1503, Pub. L. 108–11, 117 Stat. 559; E.O. 12058, 43 FR 20947, 3 CFR, 1978 Comp., p. 179; E.O. 12851, 58 FR 33181, 3 CFR, 1993 Comp., p. 608; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Presidential Determination 2003–23 of May 7, 2003, 68 FR 26459, May 16, 2003; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014); Notice of November 7, 2014, 79 FR 67035 (November 12, 2014).

- 8. Section 742.6 is amended by adding paragraph (b)(5) to read as follows:

§ 742.6 Regional stability.

* * * * *

- (b) * * *

(5) *Licensing policy for cybersecurity items*. Applications for exports, reexports and transfers of cybersecurity items, *i.e.*, those controlled by ECCNs 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items), 4D004, 4E001.a (“required” for 4A005, 4D001.a (“specially designed” or modified for 4A005 or 4D004 items) or 4D004 items), 4E001.c, 5A001.j, 5B001.a (“specially designed” for 5A001.j items), 5D001.a (“specially designed” or modified for 5A001.j items), 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) or 5E001.a (“required” for 5A001.j, 5B001.a, 5D001.a (“specially designed” or modified for 5A001.j items) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a items) items), controlled for RS will be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, “foreign commercial

partners' located in Country Group A:5, Government end users in Australia, Canada, New Zealand or United Kingdom and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including the foreign policy interest of promoting the observance of human rights throughout the world, except that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities. Any "information security" functionality incorporated in the cybersecurity item will also receive a focused case-by-case review for reasons of Encryption Items (EI) control.

Note to paragraph (b)(5): A 'foreign commercial partner' means a foreign-based non-governmental end-user that has a business need to share the proprietary information of the U.S. company and is contractually bound to the U.S. company (e.g., has an established pattern of continuing or recurring contractual relations). In addition to the information required in § 748.3(c)(1), (c)(2) and paragraph (z) of Supplement No. 2 to part 748 of the EAR, you must explain in a letter of explanation how the end user meets the criteria of a 'foreign commercial partner' and how the end user will safeguard the items from unauthorized transfers (in-country) and reexports.

* * * * *

PART 748—[AMENDED]

■ 9. The authority citation for part 748 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

■ 10. Section 748.8 is amended by adding paragraph (z) to read as follows:

§ 748.8 Unique application and submission requirements.

* * * * *

(z) Cybersecurity Items.

■ 11. Supplement No. 2 is amended by adding paragraph (z) to read as follows:

Supplement No. 2 to Part 748—Unique Application and Submission Requirements

* * * * *

(z) *Cybersecurity items.* For license applications to export, reexport, transfer (in-country) cybersecurity items, *i.e.*, ECCNs 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004 items), 4D004, 4E001.a ("required" for 4A005, 4D001.a ("specially designed" or modified for 4A005 or 4D004) or 4D004 items), 4E001.c, 5A001.j,

5B001.a ("specially designed" for 5A001.j items), 5D001.a ("specially designed" or modified for 5A001.j items), 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) or 5E001.a ("required" for 5A001.j, 5B001.a, 5D001.a ("specially designed" or modified for 5A001.j items) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a items) items) you must follow the unique application requirements set forth in this paragraph (z). If the cybersecurity item has encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, all encryption registration and review requirements must be separately completed with BIS and the ENC Encryption Request Coordinator, Ft. Meade, MD, before license applications for a cybersecurity item will be considered, see §§ 740.17 and 742.15 of the EAR.

(1) In block 9 of the application (Special Purpose) indicate the phrase "Cybersecurity Item." In addition to the information required by § 748.3(b) of the EAR, submit the following information in a letter of explanation:

(i) Whether the cybersecurity item has encryption or other "information security" functionality, Encryption Registration Number (ERN) and encryption Commodity Classification Application Tracking System (CCATS) number(s);

(ii) Whether the cybersecurity item has been previously classified or included in a license application submitted on or after May 20, 2015 for which all requirements of this section (including the questions set forth in paragraph (z)(1)(iii) of this section) have been satisfied. If so, then provide the Commodity Classification Automated Tracking System (CCATS) number(s) or issued license number(s).

(iii) If the cybersecurity item has not been previously classified or included in a license application, then:

(A) Describe the cybersecurity functions and user interfaces (e.g., Application Programming Interfaces (APIs), Command Line Interfaces (CLIs) or Graphical User Interfaces (GUIs)) that are implemented and/or supported. Explain which are for internal use private to the developer of the product, and/or which are for use by the customer or other operator.

(B) Describe the cybersecurity functionality (including as related to "intrusion software") that is provided by third-party frameworks, platforms, tools, modules or components (if any). Identify the manufacturers of the cybersecurity items, including specific part numbers and version information as needed to describe the item. As applicable, describe whether the third-party cybersecurity software is statically or dynamically linked.

(C) For items related to "intrusion software," describe how rootkit or zero-day exploit functionality is precluded from the item. Otherwise, for items that incorporate or otherwise support rootkit or zero-day exploit functionality, this must be explicitly stated in the application.

(2) Upon request, include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.

PART 772 [AMENDED]

■ 12. The authority citation for part 772 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

■ 13. Section 772.1 is amended by adding the term "Intrusion software" in alphabetic order to read as follows:

§ 772.1 Definitions of terms as used in the Export Administration Regulations (EAR).

* * * * *

Intrusion software. (Cat 4) "Software" "specially designed" or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device, and performing any of the following:

- (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
- (b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes: 1. "Intrusion software" does not include any of the following:

- a. *Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;*
- b. *Digital Rights Management (DRM) "software";* or
- c. *"Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.*

2. *Network-capable devices include mobile devices and smart meters.*

Technical Notes: 1. 'Monitoring tools': "software" or hardware devices, that monitor system behaviors or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

* * * * *

PART 774 [AMENDED]

■ 14. The authority citation for part 774 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; 10 U.S.C. 7420; 10 U.S.C. 7430(e); 22 U.S.C. 287c, 22 U.S.C. 3201 *et seq.*; 22 U.S.C. 6004; 30 U.S.C. 185(s), 185(u); 42 U.S.C. 2139a; 42 U.S.C. 6212; 43 U.S.C. 1354; 15 U.S.C. 1824a; 50 U.S.C. app. 5; 22

U.S.C. 7201 *et seq.*; 22 U.S.C. 7210; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

**Supplement No. 1 to Part 774—
[Amended]**

■ 15. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4 is amended by adding ECCN 4A005 after ECCN 4A004 to read as follows:

**Supplement No. 1 to Part 774—The
Commerce Control List**

* * * * *

4A005 “Systems,” “equipment,” or “components” therefor, “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”.

License Requirements

Reason for Control: NS, RS, AT

<i>Control(s)</i>	<i>Country chart (see supp. No. 1 to part 738)</i>
NS applies to entire entry.	NS Column 1
RS applies to the entire entry.	RS Column 1
AT applies to entire entry.	AT Column 1

License Requirement Note: *All license applications for 4A005 must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A
GBS: N/A
CIV: N/A

Special Conditions for STA

STA: License Exception STA may not be used to export, reexport, or transfer (in-country) commodities controlled by ECCN 4A005 to any destination.

List of Items Controlled

Related Controls: (1) “Systems”, “equipment” and “components” described under ECCN 4A005 are classified under this ECCN, even if the “systems”, “equipment” or “components” are designed or modified to use “cryptography” or cryptanalysis. (2) See Categories XI(b) and XIII in the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and

the U.S. Munitions List (22 CFR part 121). (3) See also ECCN 4D001.a (“development” and “production” “software”), 4D004 and 4E001.a and .c.

Related Definitions: See § 772.1 of this EAR for the definition of “intrusion software.”

Items: The list of items controlled is contained in the ECCN heading.

■ 16. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4, ECCN 4D001 is amended by:

- a. Revising the Reason for Control paragraph in the License Requirements section;
- b. Adding an entry for “RS” after the entry for “NS” in the table in the License Requirements section;
- c. Removing the NP note after the table in the License Requirements section and adding in its place a License Requirement Note;
- d. Revising the TSR paragraph in the List Based License Exceptions section;
- e. Revising the Special Conditions for STA section;
- f. Revising the Related Controls paragraph in the List of Items Controlled section;
- g. Revising Items paragraph a. The revisions and addition read as follows:

**4D001 “Software” as follows (see List of
Items Controlled).**

License Requirements

Reason for Control: NS, RS, CC, AT

<i>Control(s)</i>	<i>Country chart (see supp. No. 1 to part 738)</i>
RS applies to 4D001.a (if “specially designed” or modified for 4A005 or 4D004).	RS Column 1

License Requirement Note: *All license applications for 4D001.a (if “specially designed” or modified for 4A005 or 4D004) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

* * * * *

TSR: Yes, except for: (1) “software” “specially designed” or modified for the

“development” or “production” of commodities with an “Adjusted Peak Performance” (“APP”) exceeding 1.0 WT; or (2) “software” if “specially designed” or modified for the “development” or “production” of commodities or “software” specified by ECCNs 4A005 or 4D004.

* * * * *

Special Conditions for STA

STA: License Exception STA may not be used to: (1) Ship or transmit “software” “specially designed” or modified for the “development” or “production” of equipment specified by ECCN 4A001.a.2 or for the “development” or “production” of “digital computers” having an ‘Adjusted Peak Performance’ (“APP”) exceeding 1.0 Weighted TeraFLOPS (WT) to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); or (2) ship or transmit “software” “specially designed” or modified for the “production” or “development” of commodities or “software” specified by ECCNs 4A005 or 4D004, to any destination.

List of Items Controlled

Related Controls: (1) “Software” described under ECCN 4D001 (if “specially designed” or modified for 4A005 or 4D004) is classified under this ECCN, even if the “software” is designed or modified to use “cryptography” or cryptanalysis. (2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121).

* * * * *

Items: a. “Software” “specially designed” or modified for the “development” or “production”, of equipment controlled by 4A001, 4A003, 4A004, 4A005 or “software” controlled by 4D (except 4D980, 4D993 or 4D994).

* * * * *

■ 17. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4 is amended by adding ECCN 4D004 after ECCN 4D002 to read as follows:

4D004 “Software” “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”.

License Requirements

Reason for Control: NS, RS, AT

<i>Control(s)</i>	<i>Country chart (see supp. No.1 to part 738)</i>
NS applies to entire entry.	NS Column 1
RS applies to entire entry.	RS Column 1
AT applies to entire entry.	AT Column 1

License Requirement Note: *All license applications for 4D004 must include the information required in Supplement No. 2 to part 748 of this EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other*

"information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

CIV: N/A
TSR: N/A

Special Conditions for STA

STA: License Exception STA may not be used to export, reexport, or transfer (in-country) "software" controlled by ECCN 4D004 to any destination.

List of Items Controlled

Related Controls: (1) "Software" described under ECCN 4D004 is classified under this ECCN, even if the "software" is designed or modified to use "cryptography" or cryptanalysis. (2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121). (3) See also ECCN 4E001.a.

Related Definitions: See § 772.1 of the EAR for the definition of "intrusion software."

Items: The list of items controlled is contained in the ECCN heading.

18. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 4, ECCN 4E001 is amended by:

- a. Revising the Reasons for Control paragraph in the License Requirements section;
b. Adding an entry for "RS" after the entry for "MT" in the table in the License Requirements section;
c. Removing the NP note after the table in the License Requirements section and adding in its place a License Requirement Note;
d. Revising the TSR paragraph in the List Based License Exceptions section;
e. Revising the Special Conditions for STA section;
f. Revising the Related Controls and Related Definitions paragraphs in the List of Items Controlled section;
g. Adding paragraph c to the Items paragraph of the List of Items Controlled section.

The revisions and additions read as follows:

4E001 "Technology" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, MT, RS, CC, AT

Table with 2 columns: Control(s), Country chart (see supp. No. 1 to part 738)

Table with 2 columns: Control(s), Country chart (see supp. No. 1 to part 738). Includes License Requirement Note and License Based License Exceptions.

License Requirement Note: All license applications for 4E001.a "technology" (if "required" for 4A005, 4D001.a (if "specially designed" or modified for 4A005 or 4D004) and if "required" for 4E001.c must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

Table with 2 columns: Control(s), Country chart (see supp. No. 1 to part 738). Includes License Based License Exceptions and Special Conditions for STA.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "technology" according to the General Technology Note for the "development" or "production" of any of the following equipment or "software": a. Equipment specified by ECCN 4A001.a.2; b. "Digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 1.0 Weighted TeraFLOPS (WT); or c. "software" specified in the License Exception STA paragraph found in the License Exception section of ECCN 4D001 to any of the destinations listed in Country Group A:6 (See Supplement No. 1 to part 740 of the EAR); or to ship any "technology" specified by 4E001.a "required" for "commodities" in 4A005 or "software" in 4D001.a (if "specially designed" or modified for 4A005 or 4D004), 4D004, or by 4E001.c, to any destination.

List of Items Controlled

Related Controls: (1) "Technology" described under ECCN 4E001.a ("required" for equipment in 4A005 or "software" in 4D001.a (if "specially designed" or modified for 4A005 or 4D004) or 4E001.c is classified under this ECCN, even if it includes "technology" for the "development" or "production" of cryptographic or cryptanalytic items. (2) See also the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120 through 130) and the U.S. Munitions List (22 CFR part 121).

Related Definitions: See § 772.1 for the definition of "intrusion software."

Items: * * *

c. "Technology" "required" for the "development" of "intrusion software".

- 19. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5A001 is amended by:
a. Revising the Reason for Control paragraph in the License Requirements section;
b. Revising the first entry in the table in the License Requirements section;
c. Adding an entry for "RS" after the second entry in the table in the License Requirements section;
d. Adding a License Requirement Note after the table in the License Requirements section;
e. Revising the List Based License Exceptions section;
f. Revising the Special Conditions for STA section;
g. Revising the Related Controls paragraph of the List of Items Controlled section; and
h. Adding paragraph j to the Items paragraph of the List of Items Controlled section.

The revisions and additions read as follows:

5A001 Telecommunications systems, equipment, "components" and "accessories," as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Table with 2 columns: Control(s), Country chart (see supp. No. 1 to part 738). Includes License Requirements and License Based License Exceptions.

License Requirement Note: All license applications for cybersecurity items (5A001.j) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality

classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

* * * * *

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: N/A for 5A001.a, .b.5, .e, .f, .h, and .j; \$5000 for 5A001.b.1, .b.2, .b.3, .b.6, .d, and .g; \$3000 for 5A001.c.
 GBS: Yes, except 5A001.a, .b.5, .e, .f, .h, and .j.
 CIV: Yes, except 5A001.a, .b.3, .b.5, .e, .f, .h, and .j.

Special Conditions for STA

STA: License Exception STA may not be used to ship any commodity in 5A001.b.3, .b.5, or .h to any of the destinations listed in Country Group A:6 (See Supplement No. 1 to part 740 of the EAR), or to ship any commodity in 5A001.j to any destination.

List of Items Controlled

Related Controls: (1) See USML Category XI for controls on direction-finding “equipment” including types of “equipment” in ECCN 5A001.e and any other military or intelligence electronic “equipment” that is “subject to the ITAR.” (2) See USML Category XI(a)(4)(iii) for controls on electronic attack and jamming “equipment” defined in 5A001.f and .h that are subject to the ITAR. (3) “Systems,” “equipment” and “components” described under ECCN 5A001.j are classified under this ECCN even if the “systems,” “equipment” or “components” are designed or modified to use “cryptography” or cryptanalysis. (4) ECCN 5A001.j includes a note that explicitly excludes equipment designed for marketing purposes, quality of service (QoS) or quality of experience (QoE) purposes. The intent of the entry is to capture only products that are not “specially designed” for legitimate network operator functions. The control has very specific parameters and includes only systems or equipment that perform all five of the capabilities listed in 5A001.j below. Equipment that is not described in the new ECCN 5A001.j entry because it does not have all five capabilities required is likely to be described in ECCNs 5A002 or 5A992 if it has encryption functionality, or ECCNs 5A991 or 4A994 if it does not. However, such equipment may not be sold separately with knowledge that it will be combined with other equipment to comprise a system described in new paragraph ECCN 5A001.j. (see § 764.2(h) of the EAR) (5) See also 5A101, 5A980, and 5A991.

* * * * *

Items: * * *

j. IP network communications surveillance “systems” or “equipment”, and “specially designed” components therefor, having all of the following:

j.1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):

j.1.a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498–1));

j.1.b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and

j.1.c. Indexing of extracted data; and
 j.2. Being “specially designed” to carry out all of the following:

j.2.a. Execution of searches on the basis of ‘hard selectors’; and

j.2.b. Mapping of the relational network of an individual or of a group of people.

Note: 5A001.j does not apply to “systems” or “equipment”, “specially designed” for any of the following:

- a. Marketing purpose;
- b. Network Quality of Service (QoS); or
- c. Quality of Experience (QoE).

Technical Note: ‘Hard selectors’: data or set of data, related to an individual (e.g., family name, given name, email or street address, phone number or group affiliations).

■ 20. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5B001 is amended by:

■ a. Revising the Reasons for Control paragraph of the License Requirements section;

■ b. Revising the table in the License Requirements section;

■ c. Adding a License Requirement Note after the table in the License Requirements section;

■ d. Revising the List Based License Exceptions section; and

■ e. Revising the Special Conditions for STA section.

The revisions and addition to read as follows:

5B001 Telecommunication test, inspection and production equipment, “components” and “accessories,” as follows (See List of Items Controlled).

License Requirements

Reason for Control: NS, RS, AT

Control(s)	Country chart (see supp. No. 1 to part 738)
NS applies to 5B001.a equipment, “components” and “accessories” “specially designed” for 5A001.j.	NS Column 1
NS applies to entire entry (except 5B001.a for 5A001.j).	NS Column 2
RS applies to 5B001.a equipment, “components” and “accessories” “specially designed” for 5A001.j.	RS Column 1

Control(s) Country chart
(see supp. No. 1 to part 738)

AT applies to entire entry. AT Column 1

License Requirement Note: All license applications for cybersecurity items (5B001.a equipment, “components” and “accessories” “specially designed” for 5A001.j) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

* * * * *

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

LVS: \$5000, except N/A for 5B001.a (for 5A001.f.1 or .j)
 GBS: Yes, except for 5B001.a (for 5A001.f.1 or .j)
 CIV: Yes, except for 5B001.a (for 5A001.f.1 or .j)

Special Conditions for STA

STA: License Exception STA may not be used to ship 5B001.a equipment and “specially designed” “components” or “accessories” therefor, “specially designed” for the “development” or “production” of equipment, functions or features specified by ECCN 5A001.b.3, .b.5 or .h to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR), or to ship any commodity in 5B001.a for equipment or systems specified by 5A001.f.1, or .j to any destination.

* * * * *

■ 21. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, ECCN 5D001 is amended by:

■ a. Revising the Reasons for Control paragraph in the License Requirements section;

■ b. Adding an entry for “RS” after the entry for “NS” in the table in the License Requirements section;

■ c. Adding a License Requirement Note after the table in the License Requirements section;

■ d. Revising the List Based License Exceptions section;

■ e. Revising the Special Conditions for STA section; and

■ f. Revising the Related Controls paragraph in the List of Items Controlled section.

The revisions and additions read as follows:

5D001 “Software” as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Control(s)	Country chart (see supp. No. 1 to part 738)
* * * * *	
RS applies to 5D001.a "software" "specially de- signed" or modified for 5A001.j, and 5D001.c "software" "specially de- signed" or modified for 5A001.j or 5B001.a.	RS Column 1
* * * * *	

License Requirement Note: All license applications for cybersecurity items (5D001.a "software" "specially designed" or modified for 5A001.j, and 5D001.c "software" "specially designed" or modified for 5A001.j or 5B001.a) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

* * * * *

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

CIV: Yes, except for "software" controlled by 5D001.a and "specially designed" or modified for the "development" or "production" of items controlled by 5A001.b.5, 5A001.f.1, 5A001.h and 5A001.j.

TSR: Yes, except for exports and reexports to destinations outside of those countries listed in Country Group A:5 (See Supplement No. 1 to part 740 of the EAR) of "software" controlled by 5D001.a and "specially designed" or modified for items controlled by 5A001.b.5, 5A001.f.1, 5A001.h and 5A001.j.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit 5D001.a "software" "specially designed" or modified for the "development" or "production" of equipment, functions or features, specified by ECCN 5A001.b.3, .b.5, .f.1, .h or .j; and for 5D001.b. for "software" "specially designed" or modified to support "technology" specified by the STA paragraph in the License Exception section of ECCN 5E001 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); and for 5D001.c. for "software" "specially designed" or modified to provide characteristics, functions or features of equipment or

systems classified under ECCNs 5A001.f.1 or .j, or 5B001.a (for 5A001.f.1 or .j)).

List of Items Controlled

Related Controls: (1) "Software" described under ECCN 5D001.a or .c (if "specially designed" or modified for 5A001.j) is classified under this ECCN, even if the "software" is designed or modified to use "cryptography" or cryptanalysis. (2) See also 5D980 and 5D991.

- * * * * *
- 22. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5, Part 1, ECCN 5E001 is amended by:
 - a. Revising the Reasons for Control paragraph in the License Requirements section;
 - b. Adding an entry for "RS" after the entry for "NS" in the table in the License Requirements section;
 - c. Adding a License Requirement Note after the table in the License Requirements section;
 - d. Revising the TSR paragraph in the List Based License Exceptions section;
 - e. Revising the Special Conditions for STA section; and
 - f. Adding paragraph (3) to the Related Control paragraph in the List of Items Controlled section.

The revisions and additions read as follows:

5E001 "Technology" as follows (see List of Items Controlled).

License Requirements

Reason for Control: NS, RS, SL, AT

Control(s)	Country chart (see supp. No. 1 to part 738)
* * * * *	
RS applies to 5E001.a for commodities controlled under 5A001.j or "software" controlled under 5D001.a (if "specially designed" or modified for 5A001.j), and 5D001.c (if "specially designed" or modified for 5A001.j or 5B001.a) for RS reasons.	RS Column 1
* * * * *	

License Requirement Note: All license applications for cybersecurity items (5A001.j or "software" controlled under 5D001.a (if "specially designed" or modified for 5A001.j), and 5D001.c (if "specially designed" or modified for 5A001.j or 5B001.a)) must include the information required in Supplement No. 2 to part 748 of the EAR, paragraph (z). Also, all such cybersecurity items using or incorporating

encryption or other "information security" functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.

* * * * *

List Based License Exceptions (See Part 740 for a Description of All License Exceptions)

* * * * *

TSR: Yes, except: N/A for "technology" controlled by 5E001.a if "required" for the "development" or "production" of items controlled by 5A001.f.1 or .j, 5D001.a (if "specially designed" or modified for 5A001.f.1 or .j) or 5D001.c (if "specially designed" or modified for 5A001.j or 5B001.a) to any destination; or for exports or reexports to destinations outside of those countries listed in Country Group A:5 (See Supplement No. 1 to part 740 of the EAR) of "technology" controlled by 5E001.a for the "development" or "production" of the following: (1) Items controlled by 5A001.b.5 or 5A001.h; or (2) "Software" controlled by 5D001.a that is "specially designed" or modified for the "development" or "production" of equipment, functions or features controlled by 5A001.b.5 or 5A001.h.

Special Conditions for STA

STA: License Exception STA may not be used to ship or transmit "technology" according to the General Technology Note for the "development" or "production" of equipment, functions or features specified by 5A001.b.3, .b.5 or .h; or for "software" in 5D001.a that is specified in the STA paragraph in the License Exception section of ECCN 5D001 to any of the destinations listed in Country Group A:6 (See Supplement No.1 to part 740 of the EAR); or to ship any "technology" in 5E001.a if "required" for any commodity in 5A001.f.1 or .j, or if "required" for any "software" in 5D001.a or .c ("specially" or modified designed for any commodity in 5A001.f.1 or .j or 5B001.a ("specially designed" for 5A001.f.1 or .j)), to any destination.

List of Items Controlled

Related Controls: * * * (3) "Technology" described under ECCN 5E001.a if "required" for "systems," "equipment" or "components" classified under 5A001.j or "software" classified under 5D001.a ("specially designed" or modified for 5A001.j) or 5D001.c ("specially designed" or modified for 5A001.j or 5B001.a) is classified under this ECCN even if it includes "technology" for the "development" or "production" of cryptographic or cryptanalytic items.

* * * * *

- 23. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5A002 is amended by adding paragraph (4) to the Related Controls paragraph in the List of Items Controlled section to read as follows:

5A002 “Information security” systems, equipment “components” therefor, as follows (see List of Items Controlled).

* * * * *

List of Items Controlled

Related Controls: * * * (4) “Systems,” “equipment” and “components” described under ECCNs 4A005 or 5A001.j are classified under ECCNs 4A005 or 5A001.j, even if the “systems,” “equipment” or “components” are designed or modified to use “cryptography” or cryptanalysis.

* * * * *

■ 24. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5D002 is amended by adding paragraph (3) to the Related Controls paragraph in the List of Items Controlled section to read as follows:

5D002 “Software” as follows (see List of Items Controlled).

* * * * *

List of Items Controlled

Related Controls: * * * (3) “Software” described under ECCN 4D001.a (“specially designed” or modified for 4A005 or 4D004), 4D004, 5D001.a (“specially designed” or modified for 5A001.j) or 5D001.c (“specially designed” or modified for 5A001.j or 5B001.a) is classified under those ECCNs, even if the “software” is designed or modified to use “cryptography” or cryptanalysis.

* * * * *

■ 25. In Supplement No. 1 to Part 774 (the Commerce Control List), Category 5 Part 2, ECCN 5E002 is amended by revising the Related Controls paragraph in the List of Items Controlled section to read as follows:

5E002 “Technology” as follows (see List of Items Controlled).

* * * * *

List of Items Controlled

Related Controls: (1) See also 5E992. This entry does not control “technology” “required” for the “use” of equipment excluded from control under the Related Controls paragraph or the Technical Notes in ECCN 5A002 or “technology” related to equipment excluded from control under ECCN 5A002. This “technology” is classified as ECCN 5E992. (2) “Technology” described under ECCN 4E001.a (“required” for equipment in 4A005 or “software” in 4D004), 4E001.c, or 5E001.a (“required” for 5A001.j or 5D001.a) that is designed or modified to use “cryptography” or cryptanalysis is classified under ECCNs 4E001.a or .c, or ECCN 5E001.a, respectively.

* * * * *

Dated: May 11, 2015.

Kevin J. Wolf,

Assistant Secretary for Export Administration.

[FR Doc. 2015–11642 Filed 5–19–15; 8:45 am]

BILLING CODE 3351–33–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 514

[Docket No. FDA–2012–N–0447; 0910–AG45]

Antimicrobial Animal Drug Sales and Distribution Reporting

AGENCY: Food and Drug Administration, HHS.

ACTION: Proposed rule.

SUMMARY: The Animal Drug User Fee Amendments of 2008 (ADUFA) amended the Federal Food, Drug, and Cosmetic Act (the FD&C Act) to require that sponsors of approved or conditionally approved applications for new animal drugs containing an antimicrobial active ingredient submit an annual report to the Food and Drug Administration (FDA or Agency) on the amount of each such ingredient in the drug that is sold or distributed for use in food-producing animals, and further requires FDA to publish annual summary reports of the data it receives from sponsors. At this time, FDA is issuing proposed regulations for the administrative practices and procedures for animal drug sponsors who must report under this law. This proposal also includes an additional reporting provision intended to enhance FDA’s understanding of antimicrobial animal drug sales intended for use in specific food-producing animal species.

DATES: Submit either electronic or written comments on the proposed rule by August 18, 2015. Submit comments on information collection issues under the Paperwork Reduction Act of 1995 (the PRA) by June 19, 2015 (see the “Paperwork Reduction Act of 1995” section of this document).

ADDRESSES: You may submit comments by any of the following methods, except that comments on information collection issues under the PRA must be submitted to the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB) (see the “Paperwork Reduction Act of 1995” section).

Electronic Submissions

Submit electronic comments in the following way:

- Federal eRulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.

Written Submissions

Submit written submissions in the following way:

- Mail/Hand delivery/Courier (for paper submissions): Division of Dockets Management (HFA–305), Food and Drug Administration, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

Instructions: All submissions received must include the Docket No. FDA–2012–N–0447 for this rulemaking. All comments received may be posted without change to <http://www.regulations.gov>, including any personal information provided. For additional information on submitting comments, see the “Comments” heading of the **SUPPLEMENTARY INFORMATION** section.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov> and insert the docket number, found in brackets in the heading of this document, into the “Search” box and follow the prompts and/or go to the Division of Dockets Management, 5630 Fishers Lane, Rm. 1061, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT: Neal Bataller, Center for Veterinary Medicine (HFV–210), Food and Drug Administration, 7519 Standish Pl., Rockville, MD 20855, 240–276–9062, Neal.Bataller@fda.hhs.gov.

SUPPLEMENTARY INFORMATION:

Executive Summary

Purpose of Proposed Rule

Section 105 of ADUFA (ADUFA 105) amended section 512 of the FD&C Act (21 U.S.C. 360b) to require that sponsors of approved or conditionally approved applications for new animal drugs containing an antimicrobial active ingredient submit an annual report to FDA on the amount of each such ingredient in the drug that is sold or distributed for use in food-producing animals. ADUFA 105 also requires FDA to publish annual summary reports of the data it receives. In accordance with the new law, sponsors of the affected antimicrobial new animal drug products began submitting their sales and distribution data to FDA on an annual basis, and FDA published summaries of such data for each calendar year beginning with 2009. The purpose of this rulemaking is to amend the Agency’s existing records and reports regulation in part 514 (21 CFR part 514) to incorporate the sales and distribution data reporting requirements specific to antimicrobial new animal drugs that were added to the FD&C Act by ADUFA 105. This proposal also includes an additional reporting provision intended to further enhance FDA’s understanding of antimicrobial animal drug sales

Intrusion and Surveillance Items

1. Does the rule BIS is proposing control “intrusion software”, malware, exploits, etc.?

No, the proposed rule would not control any "intrusion software," which may also be referred to as malware or exploits. The Category 4 control entries would control the command and delivery platforms for generating, operating, delivering, and communicating with "intrusion software". It would also control the technology for developing "intrusion software," but it does not control the "intrusion software" itself.

Thus, transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware would not be included in the new control list entries and would not require a license under the proposed rule.

2. Doesn't the rule potentially criminalize hacking?

No. The rule would control the export of hardware and software delivery tools, as well as the export of technical data for developing exploits ("intrusion software"). The rule as proposed would not control the export of exploits to a target system since "intrusion software" would not be controlled. Also, the Export Administration Regulations (EAR) do not control services, only the export of commodities, software and technology. Thus, "hacking", as that term is generally understood, does not fall under the jurisdiction of the EAR, except to the extent there is an associated export of hardware, software, or technical data.

3. Does the rule inadvertently capture defensive products as well as offensive products?

The proposed rule would control the command and delivery platforms "specially designed" or modified for generating, operating, delivering, or communicating with "intrusion software" as defined in the EAR. As noted in the preamble to the proposed rule, some penetration testing products marketed as defensive products meet the technical description of such command and delivery platforms in the new control list entries. BIS is not aware of other defensive products that would be caught by the proposed rule, but would welcome comments on this. If penetration testing products are determined to be described in the Category 4 control list entries, they will be deleted from the list of products eligible for export under License Exception ENC (section 740.17(b)(2)(i)(F)).

4. Will the rule control vulnerability research as well as research on exploits?

The rule would control the export of technology for the "development" of "intrusion software", as well as the technology for the "development" or "production" of the command and delivery platforms themselves. A license would not be required simply to conduct research or analyze code, unless there was an associated transfer or deemed export of controlled technology, executable software, or source code.

As a clarification, the proposed rule would control the following, among other things:

1. Information "required for" developing, testing, refining, and evaluating "intrusion software", in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information.
2. Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.

3. The development or production of the command and delivery platform itself.

The proposed rule would not control the following:

1. Information on how to search for, discover or identify a vulnerability in a system, including vulnerability scanning;
2. Information about the vulnerability, including causes of the vulnerability; and
3. Information on testing the vulnerability, including 'fuzzing' or otherwise trying different inputs to determine what happens; and
4. Information on analyzing the execution or functionality of programs and processes running on a computer, including decompiling or disassembling code and dumping memory.

In addition, there are two further limitations to controls on technology:

First, not all malware and exploits meet the definition of "intrusion software". The definition specifies only intrusion software that is capable of extracting or modifying data or modifying the standard execution path of software in order to allow the execution of externally provided instructions. Thus, technology for the development of malware that is designed to do other things, such as damage or destroy systems or infrastructure, would not be controlled under the proposed rule.

Second, the only technology controlled is the technology that is "required for" and peculiarly responsible for achieving or exceeding the control level. See BIS's 3/25/14 advisory opinion at <http://www.bis.doc.gov/index.php/policy-guidance/advisory-opinions>.

Third, export controls do not apply to any technology or software that is "published" or otherwise made publicly available.

Thus, only that part of the technology that is peculiarly responsible for meeting the definition of "intrusion software" , and is not publicly available, would be controlled.

As part of the request for comments, BIS is seeking comments from the public on further clarifications that may be needed on this subject.

[5. Doesn't the rule expose researchers to criminal prosecution if they carry information on exploits to a public conference, unless they publish it before the conference?](#)

Under Section 734.7 of the EAR, information that is published, or released at an open conference, is not subject to the EAR. That section also specifies that it would not be an export to transfer the technical data to conference organizers with the intent that it will be published at the conference.

BIS welcomes comments on whether further clarification is needed on when information potentially subject to these rules would be considered "publicly available" and not subject to the EAR.

[6. Doesn't the rule make it easier for researchers to provide exploitable bugs to their government then to publish an exploit in order to fix and alert the world of the problem?](#)

Under Section 734.7, there are no restraints on publishing information otherwise subject to control, and no prior authorization from BIS is required. Once the information is published it is not subject to the EAR. Thus any information that is published is completely outside the scope of the EAR and the provisions of the proposed rule.

[7. Will companies be required to share their zero-day exploits with the government in order to get a license?](#)

The rule states that when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled cybersecurity functionality. Exploits that meet the definition of "intrusion software" are not controlled. Therefore, BIS would not request a company to share a zero-day exploit. Please see FAQ #15.

[8. Does the rule capture auto-updaters and anti-virus software?](#)

No. Software that permits automatic updates and anti-virus tools are not described in proposed ECCN 4D004. ECCN 4D004 software must be specially designed or modified for the generation, operation or delivery of, of communication with, "intrusion software," which is separately defined. Anti-virus software is a 'monitoring tool' that is explicitly excluded from the definition of "intrusion software. Further, software that automatically updates itself may need to interact with installed 'monitoring tools' and protective countermeasures in order to properly execute, but they are not defeating (or otherwise subverting) the system or generating, operating, delivering, or communicating with "intrusion software".

[9. Would ECCN 4E001.c be covered by the General Technology Note?](#)

Yes. Per the advisory opinion issued by BIS on 3/25/14, the GTN applies to all ECCNs controlling "technology," regardless of whether the ECCN specifically refers to the GTN or uses the term "required."

[10. If an IT security researcher had done an analysis on a software application to find a vulnerability in the code, had written up code to then take advantage of the vulnerability and then sent that code to an anti-virus company or the software manufacturer, would that code require an export license?](#)

No, what is described is the creation of an "exploit." Exploits are not described in the text of the proposed control list entries. The code that takes advantage of the vulnerability would not require a license. As stated above, "intrusion software" itself would not be controlled by the proposed rule.

For any associated technology for the "development" of "intrusion software", under section 734.7 of the EAR, any technical data sent to an anti-virus company or software manufacturer with the understanding that the information will be made publicly available, would not be subject to the EAR. However, "technology" that is not intended to be published would be subject to the control – see question #4.

[11. The first FAQ basically equates “intrusion software” with malware and exploits. Is this the intent?](#)

The definition of "intrusion software" is meant to include a subset of all the malware (exploits, viruses, etc.) that are out there. The definition describes only "intrusion

software" that is specially designed to extract or modify data or modify the standard execution path of software in order to allow the execution of externally provided instructions. Other types of malware, including software that only leaves evidence of a successful security breach without further compromising or controlled the system, or is designed to destroy data or systems would not be included in the definition of "intrusion software."

12. There is a reference to penetration testing products in another FAQ. Is that to say that all penetration testing products would fit the definition of "intrusion software"?

Some penetration testing products meet the description of systems, equipment or software "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software" set forth in proposed ECCNs 4A005 and 4D004. The tools that meet the entry are ones that are "specially designed" or modified to launch exploits or other malware that meet the definition of "intrusion software" – including extracting or modifying data on the system.

However, there are some tools that are used in penetration testing that are not caught by the entries because they do not do the things described in the definition. For example, tools such as port scanners, packet sniffers and protocol analyzers would not be controlled. A penetration testing tool not designed to avoid detection by 'monitoring tools' would not be controlled. Also, a vulnerability scanner, which just finds vulnerabilities in a system without actually exploiting them and extracting data, would not be captured by the proposed rule.

13. There are defensive products on the market that would probe a network for vulnerabilities (while avoiding the monitoring tools) and would then extract some sample data from the target system to prove that the vulnerability is real. However, that data extraction is benign and merely done as a proof of the vulnerability. The entire process - from the product's capabilities on what it extracts to the act of using it - is done as a defensive act. Would this be considered meet the definition of "intrusion software"?

Such products would meet the technical description of systems, equipment or software "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software" set forth in proposed ECCNs 4A005 and 4D004. It is BIS's understanding that there is no technical basis to distinguish defensive products from offensive products (i.e., a defensive product may be used offensively).

14. Is there a definition of "carrier class IP network" (for ECCN 5A001.j)?

The term "carrier class IP network" is meant to specify systems that sit at a national level (or large regional) IP backbone and handle data from an entire city or country. In terms of IP network surveillance systems, this is meant to exclude systems that can only handle smaller data streams or networks, such as those for a campus or a neighborhood. This control does not capture systems that can only analyze data from one person or a small group of people at a time. The term "carrier class IP network" was not defined because it was difficult to put precise technical parameters around this concept.

15. The answer to FAQ #1 says "exploit samples, exploit proof of concepts, or other forms of malware would not be included" yet the answer to FAQ #7 appears to keep the door open for "zero-day exploits". Can you please clarify your definition of "zero-day exploit" and

[provide discriminating characteristics to differentiate it from the "exploit samples, exploit proof of concepts" that are explicitly excluded by question 1?](#)

This is a two-part answer. First, the answer to FAQ #1 states that the proposed rule does not control the export of exploits and other forms of malware. Zero-day exploits are included in this answer. The export of zero-day exploits, however the term "zero-day" is defined, is not subject to any requirements under the proposed rule.

Second, FAQ #7 asks whether companies will be required to share their zero-day exploits with the government in order to get a license. The answer to FAQ #7 states that when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled functionality. To expand this answer, the export license requirement applies to the system, equipment, component or software that would generate, operate, deliver or communicate with an exploit. The only regulatory distinction involving zero-day exploits in the proposed rule regards the possibility that a delivery tool could either have (e.g., incorporate) or support (e.g., be 'specially designed' or modified to operate, deliver or communicate with) zero-day exploits. If the system, equipment component or software at issue has or supports zero-day or rootkit capabilities, then BIS could request the part of the software or source code that implements that capability. BIS does not anticipate receiving many, or any, export license applications for products having or supporting zero-day capabilities.

[16. Is the United States legally bound to implement the December 2013 Wassenaar Arrangement changes to its control list, or does BIS have discretion?](#)

The United States, as a Participating State in the Wassenaar Arrangement, has agreed to maintain national export controls on items included in the Wassenaar Arrangement's control lists, implemented via national legislation and/or regulation. The U.S. implementation process includes determining reason(s) for control, which carry with them license requirements by destination, licensing policy, and license exceptions.

[17. How would the proposed rule affect software used by multinational companies that monitor their overseas networks?](#)

Under the proposed rule, all exports of specified systems, equipment, components or software that would generate, operate, deliver or communicate with "intrusion software" would require an export license. There is no license exception for intra-company transfers or internal use by a company headquartered in the United States under the proposed rule.

[18. Security professionals use exploit toolkits \(e.g. Neosploit, Blackhole, Phoenix, Crimepack &c.\) to test patches and harden systems employing the same tools as a potential criminal adversary. Distribution and licensing of such toolkits is tightly controlled in order to preserve their offensive edge. When security professionals succeed in accessing or acquiring these toolkits, they often share with one another across corporate and international boundaries; would such sharing of exploit toolkits be subject to control?](#)

Exploit toolkits would be described in proposed ECCN 4D004 if they are "specially designed" or modified for the generation of "intrusion software." There are no end user or end use license exceptions in the proposed rule.

19. Security research is intellectually demanding, skilled work. Corporate entities recognize this both by compensating their contracted security professionals accordingly, and by compensating independent researchers who find and report vulnerabilities in their digital infrastructure. These 'bug bounties' are not generally awarded in the absence of a fully-elaborated proof of concept, which is functionally identical to an 'exploit'; the vulnerability must be shown to be exploitable and its severity level should be made known to the vendor. What, if any, implications does the proposed rule hold for: i. 'Silent' disclosures, in which the researcher may be compensated, but neither the vendor nor the researcher publicly disclose ('publish') the vulnerability? (Most often a vendor choice.); ii. Disclosures in which a vulnerability is made public, but its proof of concept is not; iii. Disclosure of any stripe made through an intermediary (i.e. to HackerOne or via a legal representative)?

First, the proposed rule would only apply to exports and reexports of software described in the new control list entries. Domestic commerce in exploits is not subject to the requirements of the Export Administration Regulations.

Second, in none of the scenarios above would the exploit or proof of concept be considered to be software described in the new control list entries. See questions 4 and 10.

Finally, if an export is at issue, it is possible that certain technology associated with the exploit would be "technology required for the development or production of intrusion software" under proposed ECCN 4E001.c. As stated in the answer to FAQ #10, any technical data that is transferred with the intent that it be published would not be controlled. However, as the

question recognizes, not all technical data is intended to be made public, and some of it may be controlled.

20. When vulnerabilities are found and proofs of concept developed from flaws in proprietary systems, does this have bearing on the classification of security research as 'fundamental'? What about when access to that proprietary system is neither specifically authorized, nor unauthorized by the vendor?

No, whether the system is proprietary or open source, and whether the access to the system is authorized by the vendor, does not affect whether the security research is "fundamental research." If the research is ordinarily published and shared broadly within the scientific community, it is "fundamental research." If the results of the research ordinarily are restricted for proprietary reasons, it is not. The answer to question 19 above describes a situation when such research would not be "fundamental research."

21. Could BIS explain the regulatory difference between an open-source security tools (e.g. Metasploit, Kali Linux), and a proprietary surveillance platform (e.g. FinFisher) which may come packaged with open-source tools?

Open source security tools such as those referenced that can be downloaded by anyone are not subject to the Export Administration Regulations . Proprietary tools that package and control such open source tools are subject to the regulations and may be described in the new control list entries.

22. BIS has adopted the definition of ‘intrusion software’ from the Wassenaar Arrangement language, but has elsewhere indicated a policy of ‘presumptive denial’ for cybersecurity items ‘that incorporate or otherwise support rootkit or zero-day exploit functionality’. Could BIS explain what threshold of severity is meant to be indicated by ‘rootkit or zero-day exploit functionality’, and could BIS make clear their understanding of those terms?

Rootkit and zero-day exploit functionality are features more likely to be found in offensive systems or products. A zero-day exploit is not itself controlled. However, when a rootkit or a zero-day exploit is incorporated into a product or system that is described in the new Category 4 control list entries, or if an exploit delivery tool is specially programmed to deliver or command this specialized malware, that product or system is presumed to be offensive by design.

23. In FAQ #9, BIS stated that the Wassenaar General Technology Note was incorporated into the BIS proposal. Does the Wassenaar General Software Note also apply?

The "public domain" provisions (paragraph 2) of the Wassenaar General Software Note (GSN) apply, but the "mass market" provisions (paragraph 1), do not.

Paragraph 1 of the General Software Note is implemented in the Export Administration Regulations in License Exception TSU (section 740.13(d)). The proposed rule excludes software described in the new control list entries from eligibility under this provision. This exclusion was added to the proposed rule because a similar exclusion applies to encryption software classified under ECCN 5D002, and software described in the new control list entries may incorporate encryption functionality. Software classified under ECCN 5D002 is separately eligible for decontrol to ECCN 5D992 pursuant to the provisions of section 742.15(b) for mass market encryption items. The proposed rule does not provide for any license exception eligibility for products under the new control list entries, except under License Exception GOV.

24. Would prior BIS authorization be required for a researcher to privately disclose an exploit to a vendor outside the US with the understanding that the information would NOT be published?

No. The exploit itself is not described in the new control list entries. Please see the answer to question #1. For this question, a vulnerability is a weakness in a vendor's software or hardware. Exploit code could be written to take advantage of the vulnerability or to prove that the vulnerability can be exploited. The exploit code itself may be considered "intrusion software." Neither the disclosure of the vulnerability nor the disclosure of the exploit code would be controlled under the proposed rule. However, information for the development of "intrusion software" that may accompany the disclosure of the exploit may be described in proposed new ECCN 4E001.c.

25. In FAQ #10, BIS states that the new implementation would not control “code that takes advantage of [a] vulnerability.” However, FAQ 4 states that “information on how to prepare the exploit for delivery” is controlled. We’re confused as to how a researcher could submit to a vendor a functional proof of concept and accompanying explanatory material that according to FAQ 10 would not be controlled without violating the restriction from FAQ 4. This assumes that the disclosure to the vendor is not intended for publication.

The functional proof of concept may be "intrusion software." The intrusion software itself is not described in the new control list entries (per FAQ #10). However, if technology "required for the development of intrusion software" (as described in the proposed control list entry ECCN 4E001.c.) exported with the functional proof of concept/"intrusion software" would be described in new control list entry ECCN 4E001.c and would, under the proposed rule, require a license to all destinations except Canada. This is what is addressed in the answer to Question #4.

[26. Mobile phone jailbreaking tools include platforms for delivering intrusion software to the phone. These generally include fully operational exploits including the delivery code. Are such tools subject to control?](#)

This response divides the question into two parts:

i) Does this regulation make it illegal to jailbreak a phone?

No. The Commerce regulation controls exports of certain software, and downloading jailbreaking software to a computer within the United States and using it to jailbreak a phone does not involve an export of software. The proposed rule does not limit the ability of owners to modify their devices.

ii) What if the jailbreak software includes a platform for delivering intrusion software to the phone--is the jailbreak software subject to control?

If particular jailbreak software did meet all the requirements for classification under ECCN 4D004 (such as a commercially sold delivery tool "specially designed" to deliver jailbreaking exploits) then it would be subject to control and a license would be required to export it from the United States. Note that if such software were "publicly available," it would not be subject to the Export Administration Regulations.

[27. In FAQ 7, BIS states companies are already required to share source code for exploits that include encryption or cryptanalysis. What about software tools that implement exploits that aren't already subject to encryption controls?](#)

The provision referred to is specific to requests to make encryption source code eligible for export under License Exception ENC. Supplement No. 6 to part 742, a questionnaire required to be submitted with requests for License Exception ENC authorization, provides that a copy of the sections of the source code that contain the encryption algorithm, key management routines and their related calls is to be included upon request. (Supp. No 6, paragraph (d)(3)). The proposed rule includes a similar provision for license applications for products that are described in the new control list entries in Supplement No. 2 to part 748, paragraph (z)(2): "Upon request, include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality."

[28. Does "publicly available" as understood by BIS include a posting on the Internet?](#)

Yes, technology or software that is generally accessible to the interested public in any form, including by Internet post, is "publicly available."

[29. Most intrusion software is designed, written, and generated in general purpose programming environments \(such as IDEs \[integrated design environments\]\). We presume that BIS has no desire to control those types of tools. However, under the](#)

[proposed rules, such environments are at least potentially within the controls. What does BIS mean when it says that "the development or production of the command and delivery platform itself" \(FAQ 1\) is controlled?](#)

General purpose tools, such as IDEs, are not described under proposed ECCN 4D004 because they are not "specially designed" for the generation of "intrusion software." Some penetration testing tools (FAQ #12) and exploit toolkits (FAQ #18) are described in proposed ECCN 4D004, as they are command and delivery platforms for "intrusion software."

[30. What does BIS mean by "modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions"?](#)

This language is part of the definition of "intrusion software" and refers to a variety of techniques to hijack, or otherwise corrupt, a legitimate (or otherwise trusted) application or process running on the computer, mobile phone or other device. This can be done to create persistence or for other purposes. Through these modifications, a remote operator (or remote command and control software) can execute commands or perform other tasks that further compromise or exploit the hacked (penetrated) device.

[31. When the 2013 Wassenaar update added controls 4.A.5, 4.D.4, 4.E.1.c, and 5.A.1.j, it subjected all these categories to the exemptions available under the "General Software Note", ensuring that software and systems "generally available to the public" were not included in the new controlled classes. Yet the proposed BIS implementation of these controls excludes "cybersecurity software" from the BIS "General Software Note" \(740.13.d\) by adding paragraph 740.13.d.2.ii. Why has BIS chosen to depart from the 2013 Wassenaar language and exclude software covered by the new controls from the "General Software Note"?](#)

Please refer to the answer to FAQ #23. The exclusion of software described in the new control list entries from License Exception TSU (the implementation of paragraph 1 of the General Software Note in the Export Administration Regulations) was added for consistency with the treatment of encryption software classified under ECCN 5D002, as it is anticipated that many items that will be classified under the new control list entries have encryption functionality and are currently classified under ECCN 5D002. However, under the proposed rule, items classified under the new control list entries will not be eligible for decontrol in the same way that ECCN 5D002 products are if they are mass marketed (pursuant to Note 3 to Category 5 part 2 of the Commerce Control List and section 742.15(b) of the Export Administration Regulations).

[32. Will technology and source code classified under the new control list entries be subject to deemed export requirements?](#)

Yes, the proposed rule does not provide for any exceptions to deemed export license requirements for release of technology and source code that will be classified under ECCNs 4D004, 4E001.a or .c, 5D001 or 5E001.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: May 20, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iyj-7mu8
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0002

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matthew Fisch

Address:

409 Cemetery Road
East Chatham, NY, 12060

Email: mfisch@kplat.com

Phone: 5184444181

Organization: Kinetic Platforms Incorporated

General Comment

See attached file(s)

Attachments

KPI_BIS_COMMENT_20150520



ADMINISTRATIVE CONTACT

PHONE +1 518 444 2151

FAX +1 928 752 4141

PO BOX 262

60 ELM STREET

SPENCERTOWN, NY 12165

**OFFICE OF MATTHEW FISCH
CHIEF TECHNOLOGY OFFICER
KINETIC PLATFORMS INCORPORATED**

409 CEMETARY ROAD

EAST CHATHAM, NY 12060

PHONE +1 518 444 4181

MFISCH@KPLAT.COM

Attention: United States Federal Industry & Security Bureau
Subject: **Comment For Public Record**
RE: BIS Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

My company strongly advises against adoption of the proposed rule to include 'intrusion software' in the list of controlled exports.

We routinely interface as part of our practice with US domestic entities looking to manage the financial risks and direct economic impacts associated with information security and risk (infosec or cyber-security).

While it is important for the United States and its allies to maintain a leading posture in the field of cyber security the class of restrictions proposed will in my view have an entirely detrimental effect to that end. Additionally it will disproportionately disadvantage domestic commercial interest where such entities depend on publicly disclosed security information.

Unlike the vast majority of current commercial software vendors (which are primarily based domestically or within allied borders); the security community (both individuals and incorporated entities) is distributed evenly across the industrialized world.

The vast majority of anti-malware and anti-virus vendors (US based or otherwise) leverage research teams around the world in the most suitable labor markets. It is likely that markets outside the US export wall will become politically unreachable for US-based infosec vendors under a restricted export regime. This would both increase the cost of these mitigative products as well as reduce the efficacy.

It has already been proven by private industry that "taking vulnerabilities off the table" with commercial bug-bounty programmes is highly effective in increasing the overall security quality of otherwise vulnerable products. Commercial web properties and software vendors now

depend on international support to support their security programmes and cannot maintain or improve their infosec postures independently.

Of those information security research community members based internationally many have voiced or otherwise indicated a disinterest in responsible disclosure under restrictive conditions. Security researchers are often motivated by perceived ethical or moral objectives in addition to financial reward; restricting information sharing to the greater international community makes responsible disclosure a less ethical choice when considering the impact to external communities. For these individuals or groups responsibly disclosing to US companies that are in turn restricted from sharing information; the black-markets for zero day vulnerabilities are an extremely profitable alternative.

Further, fragmenting the marketplace for security products and the knowledge-base of security vendors will undoubtedly hinder the overall security posture of both civilian and defense systems at home by degrading the overall quality and diversity of available tools and products.

I highly recommend the interested rule-making parties reconsider such attempts to classify cyber-security tools and knowledge of exploitation kits or methods as potential arms. While responsible researchers, vendors, and professionals will be handicapped by a limited ability to freely coordinate cross borders; nefarious actors will have no such restrictions and meet no resistance crossing borders digitally.

The only proven effective defense against information security threats is a strong investment in the strength of defenses. Do not weaken our security community.

Drafted 5/20/2015

Matthew Fisch
Chief Technology Officer
Kinetic Platforms Incorporated

PUBLIC SUBMISSION

As of: 7/10/15 12:43 PM
Received: May 20, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iyi-2v83
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0003

Comment on FR Doc # 2015-11642

Submitter Information

Name: Paul Pliska

General Comment

This is a terrible idea. Don't do it.

PUBLIC SUBMISSION

As of: 7/10/15 12:45 PM
Received: May 20, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iyp-6sde
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0004

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

This rule will do nothing more than stop the good guys (who do not want to go to jail) from defending our networks from the bad guys.

We know that the bad guys do not follow the rules. What makes it any different that they will follow this rule? Yet, this severely restricts the ability for cybersecurity personnel to use security tools to help defend networks, identify threats, etc.

In many cases, I work with security researchers all over the world identifying emerging and 0-day threats. We use the intelligence to assist our respective companies against attack. Federal LEO agencies benefit from this research from a voluntary sharing agreement (just see any number of the private / public sharing relationships that have been used to bring down cybercriminals from around the world).

Please rethink your position on this bill and allow the cybersecurity heros to continue to protect us by doing what they need to (in all lawful ways).

PUBLIC SUBMISSION

As of: 7/10/15 12:47 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iys-1979
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0005

Comment on FR Doc # 2015-11642

Submitter Information

Name: Chev Young

General Comment

I am deeply disturbed by your propols to regulate the exportation of software with "intrusive capabilities". As a developer and security researcher, I frequently exchange code with other developers around the world. If we were not able to do so, or if we had to purchase lisense to exchange certain code, than it would seriously hurt the open source community. Security researchers need to be able to share eachothers work without restriction. If this law passes, the computer security industry will likely be taken over by big corporations because of the lisense restrictions. The definition is too broad as well. Simply having a linux machine with the default programs is enough for an experienced programmer to develope his own software to intrude other systems. The security of the world's computing systems will be compromised if you start restricting who can download what simply because of they're geographic location. Finally, I am very disturbed by the mention of putting restrictions on cryptographic software. Everyone has a right to privacy, and the truth is that the US government violates the entire world's privacy every day with data collection programs. I don't see what you're trying to accomplish or prevent, I only see a future full of red tape. There is just too much that could go wrong here. Don't do this.

PUBLIC SUBMISSION

As of: 7/10/15 12:49 PM
Received: May 20, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iyf-d5qb
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0006

Comment on FR Doc # 2015-11642

Submitter Information

Name: Eric Rand

Address:

PO Box 970

Frazier Park, CA, 93225

Email: eric.rand@brownhatsecurity.com

Organization: Brown Hat Security

General Comment

Good morning;

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

a. How many additional applications would be for products that are currently eligible for license exceptions?

b. How many additional applications would be for products that currently are classified EAR99?

Answer 1: Between 50 and 50,000 - this depends entirely on how successful a year has been.

a: The majority of the above.

b: The remainder of the above.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

Answer 2: A comparable number to answer 1, depending on how successful my company is in a given year.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

Yes, significantly:

The language provided for the proposed rulemaking is highly problematic from an industry standpoint. Many of the terms used for the industry items that are proposed to be regulated are ill-defined and can be interpreted in multiple ways - a situation that lends itself to enriching lawyers while hindering the security industry.

Specifically, there is a concern amongst many in the information security industry that the rules as written can be interpreted as applying to purely defensive technologies that are essential for the safety and security of United States interests. Additionally, there is grave concern in the research community that these rules would apply to necessary and proper tools and information that they require in order to effectively secure the assets and information of United States companies.

The information security industry is organized in such a manner that licensing as has been proposed would reduce the number of effective actors significantly; in an industry that is already suffering from far greater demand than there are resources available to fill, such a situation would be catastrophic.

Additionally, while hindering legitimate security research, these proposed rules provide no disincentive to criminals and saboteurs above and beyond that which the CFAA already provides.

Bluntly, this proposed rule would negatively impact the informational security of the United States and of those corporations, persons, and agencies therein; this impact would be severe and long-lasting; and the interests of the United States as a whole will be damaged in such a lasting manner that they may never fully recover.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

This is not known; we do not have this information to hand and obtaining it may be problematic.

PUBLIC SUBMISSION

As of: 7/10/15 12:50 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iz3-9m7d
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0007

Comment on FR Doc # 2015-11642

Submitter Information

Name: Every One

General Comment

You clearly have no understanding of the technology nor a grasp of reality, not to mention no memory of history.

PUBLIC SUBMISSION

As of: 7/10/15 12:52 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iz4-ixlc
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0008

Comment on FR Doc # 2015-11642

Submitter Information

Name: Chris Houser

Address:

16 Tulane Court
Savannah, GA, 31419

Email: chris_houser@outlook.com

General Comment

As a penetration tester, I find such action reprehensible and severely shortsighted. To think that a governing agency believes that limiting the use and distribution of (in most cases) open source software is absurd given the nature of Internet access across the globe today. Worst case, this only puts tools in the hands of attackers only, while allowing organizations in countries with such silly bans to be vulnerable to zero-day attacks.

In my profession, I rely on these tools, which are created worldwide by researchers, to perform rigorous testing which is properly contracted and documented with a client. If this measure passes, it will irreparably harm the security industry, and worse yet, it will allow for future weaknesses to go undiscovered for longer - likely until actively exploited in the wild.

Thankfully, I was only a teenager when similar ridiculous bans on strong encryption led to the development of weak 'export' ciphers - something I deal with daily when advising clients to ensure their systems are not vulnerable to outsiders, outsiders in other countries, many times. Forcing this type of draconian, weak stance on security is a fatal mistake that will only lead to more high-profile breaches, more PII and cardholder data compromise, and more stupid legislation in the name of so called 'security'. One would hope that we can learn from past

mistakes and not force this down people's throats without realizing the impact down the road. I for one, certainly hope this measure dies where it is.

PUBLIC SUBMISSION

As of: 7/10/15 12:53 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iz7-g4ot
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0009

Comment on FR Doc # 2015-11642

Submitter Information

Name: James Pittman

General Comment

I am an information security practitioner, and I am generally critical of any intersection between politics and technology, since those domains of knowledge work on very different principles and vastly different timescales.

My objections to this proposal are simple in nature and reflect a healthy skepticism of both the intent and the practical implementation of it.

Firstly, the proposed action to broadly expand export controls to rapidly developing technologies not dependent upon local resources limited by the geographical boundaries identified in the proposal reveals said proposal to be fundamentally flawed. The fundamental technologies upon which the restricted technologies are built are already spread beyond the proposed geopolitical boundaries, so limiting the information (bits and bytes of software and/or the mathematical algorithms in software/firmware/hardware) will at most delay the implementation of that software or algorithm by law-abiding citizens; criminals will not be deterred by restrictions as evidenced by an Internet search of data breaches. Essentially, this proposal adds a burden of compliance without the promise of any realistic benefit.

Secondly, the nature of the targeted technologies are all too often portrayed in analogies to weapons of war, with capabilities not limited to intelligence gathering, disrupting supply chains, and actually damaging resources and personnel. As such, the proposal aims to deny these weapons to entities outside the authorized geopolitical boundaries. Unlike the nuclear arms race

where certain raw materials can be controlled (special nuclear materials like uranium, thorium, and plutonium), bits and bytes can be created from electrons anywhere; there is no need for the electron to have originated inside a specific geographical boundary. Thus exposed, this flaw highlights that the intent to control these potential technological weapons is either naive or hiding some other intent. If it fails to control the technology, then at best it will force law-abiding entities to identify themselves as users of the technologies and making them targets of surveillance or suspicion when any malicious use of these technologies is detected.

As with any regulation, a proper balance must be struck between the impact of the regulation (i.e. the burdens placed upon those who comply with it as well as the impact on the associated persons, businesses, markets, etc. that rely on the regulated individuals and businesses) with the intended benefit. In this case, the proposed benefit is a fictional increase in the control of vaguely defined technology that could serve either beneficial or malicious ends, but this technology is necessary for law-abiding entities to be able to defend themselves against possible malicious use of it.

With no clear benefit, it is trivial to demonstrate that this proposal will do more harm than good to any entity that must directly adhere to it without even considering the collateral damage. However, it is important to note that the collateral damage will be even worse in this case, since it will hamper those attempting to abide by the law while having no impact on those who would otherwise commit criminal actions. Furthermore, the effect is compounding in that the entities within the controlled geopolitical boundaries of this proposal would in effect give a competitive advantage to those outside of it, eventually causing a shift in the market (as companies move their relevant business elsewhere) and to employment (as jobs would follow the companies to more favorable locations).

In sum, this proposal should be rejected wholesale, as it will cause harm and is unlikely to produce any benefit. I would also suggest that the individuals who crafted it openly explain both the intent and logic behind it before any revisions are made.

PUBLIC SUBMISSION

As of: 7/10/15 12:54 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8iz8-edyr
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0010

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

The crypto export restrictions 20 years ago were not only ineffective, but actively harmful to America's security by enshrining extremely low standards and poor tools. The world is steal dealing with the consequences today (see the very recent LogJam bug due to EXPORT grade crypto).

Clearly, this proposal would have no positive effect. Criminals will not stop using and sharing tools, in or out of the US.

On the other hand, all legal research and development will have to move out of the US (again), leaving a lack of skill and lost jobs behind, while paradoxically bringing the state-of-the-art to more open places.

I would recommend that this proposal be reconsidered in favor of more realistic ideas.

PUBLIC SUBMISSION

As of: 7/10/15 12:57 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8izb-kfmz
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0011

Comment on FR Doc # 2015-11642

Submitter Information

Name: Randy Wyatt

General Comment

Please don't implement any new rules that aren't specified in complete detail. The import/export of certain tools and exploits are critical to the security of hosts on the internet.

How am I going to determine if my host is vulnerable to a certain exploit other than running the proof of concept? It is ridiculous to rely on the vendor which may take delayed action allowing a dangerous vector into my network.

The network intrusion tools allow me to search for ports that shouldn't be open. It allows risk assesment and allows mitigation techniques.

From a citizens perspective, it would have been nice if large companies were actively using these tools as my personal information has been compromised twice this year.

In summary, the tools should not be subject to any additional regulation that will discourage active use and free transfer of these tools.

PUBLIC SUBMISSION

As of: 7/10/15 12:59 PM
Received: May 21, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8izd-o4d1
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0012

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jack Beglinger

Address: United States,

General Comment

Like this will work. This system is broken by design. The only way you could enforce such rules is to block ALL internet connections from inside US borders to/from outside of US borders. Look at how well the "Great-Firewall-of-China" is working.

If you allow any outside US connection, a simple encrypted pipe of less than your number of bits will be just as impossible for you crack as one with more. WHY? Because an encrypted pipe can contain an encrypted pipe, that can contain an encrypted pipe, that contain ... ,, and finally encrypted data. Lets assume that each pipe is only using 64bit encrypt and is twenty level deep (2^{64} keys)*20! key sets are required. At no point will you have a clear text to know you have broken enough keys and levels, so no inspection can take place to insure ANY goals you are wanted to meet are met. If you also have the pipe also carrying normal binary or even random data just to hard, how can you tell when one type from the next?

With an open system like the internet you have lost before you began. Look at the past when Clinton Admin tried to stop high encryption by equating it to mutations. Free speech and open boarders allowed the information to "leak" by people just traveling to/from another country. Shot, with IRAN in the news, it is possible to walk in a library and read a science book to get the details of A-Bomb from the 40's. Guys, the horses have already left the barn, closing the doors will not help!

Please stop before you begin and waste tax payer's money of pork-barrel project. If the US person can think it up, so can the rest of the world. With H-1B's, we are already *teaching* the rest of world.

PUBLIC SUBMISSION

As of: 7/10/15 1:03 PM
Received: May 22, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8izk-nbig
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0013

Comment on FR Doc # 2015-11642

Submitter Information

Name: ã, °ãf-ã, § i no longer abide by it.

Address:

237 Kearny #220

San Francisco, CA, 94108

Email: noiwillnotshareitwithyou@mailinator.com

Phone: 8885551212

General Comment

Cryptographic export legislation has *never* worked.

Please, stop even attempting to introduce new legislation.

The OpenSSH project had graduate students of non-US citizenship (at least one of whom was even studying in the USA at the time) travel across geographic borders in order to continue doing legitimate research, so as to be mindful of the compliance on export regulations, and still contribute to a free, open source and commercially reusable SSH implementation.

Similar acts will occur if new legislation is introduced.

It is time to realize that the internet is now global.

Yes, it began as Engelbart's oNLine System in Menlo Park in the 1960s, and received ARPA funding from JCR Licklider to become what we now know as the internet, but it has been, and ideally, will continue to be an OPEN system, implemented with public processes, Request For

Comments and multiple vendor implementations for any meaningfully extant protocol.

Creating and subverting such processes with legislation is regressive.

As one of my colleagues phrased it: "The political processes of the United States made a lot of sense, hundreds of years ago, when the fastest way to transmit a message was sending someone on the back of a horse. We are now far past that, but our legislative processes have not kept up."

Making **any** attempt at cryptographic export regulations is folly.

I have no amendments to offer this document, because it should not exist.

It is stifling on research, education and **practical** daily operational practices of multi-trillion dollar economies globally, of which, the USA, with more than \$18 trillion dollars in **debt** is not part of any longer.

It is time to stop even attempting to stay relevant. Technologists and researchers are sick of the malignancy that has become the US governmental process, more corrupt than useful. Subjugated to bribery (though, since that is illegal, your duplicitous use of the term "lobbying" in its place, shrouds the complicit corruption with every breathe and word you utter).

Desist from even introducing, let alone passing, any legislation which would further inhibit the free flow of information.

Shutter the FCC, whose tract records, over the whole of the 20th century, did more to stifle innovation than protect it.

Those who cannot program, who cannot implement cryptographic protocols themselves, should NEVER and must not ever, pass legislation inhibiting those who can and do.

ï½œ

ã, °

ãf¬

ã, §

PUBLIC SUBMISSION

As of: 7/10/15 1:04 PM
Received: May 22, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8izt-nwyn
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0014

Comment on FR Doc # 2015-11642

Submitter Information

Name: PAWEL KRAWCZYK

Address:

57 QUEENSWAY

READING, Berkshire, United Kingdom, RG4 6SJ

Email: pawel.krawczyk@hush.com

Phone: 07879180015

General Comment

Regarding the proposed intrusion software export restrictions it's important to note that the information security research industry is primarily driven by an open scientific community. The community publishes significant number of publicly available descriptions of various attacks and computer programs used for proof-of-concept and penetration testing. Extending the export restrictions on these products would have a severe impact on the culture of scientific publication and sharing of research results. The programs implementing attacks that are either publicly known or reported to the appropriate vendors and awaiting fixes should thus NOT be covered by export controls. These controls should be thus perhaps limited to so called "zero-day vulnerabilities" which are not published after discovery, but instead traded by specialised companies and not disclosed to increase their offensive potential, and thus market value.

PUBLIC SUBMISSION

As of: 7/10/15 1:18 PM
Received: May 22, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j00-b682
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0015

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jesse Friedman

Address:

6445 Greene St

C404

Philadelphia, PA, 19119

Email: jesse@jesse.ws

General Comment

This is, quite simply, a really terrible idea. One great thing about the internet is the wide availability of security research tools. These tools encourage the advancement of security worldwide. I invite you to find a list of major web security vulnerabilities uncovered in the past decade. I bet at least half were uncovered by members of the public. Additionally, many major companies offer "bug bounty" programs, paying users to responsibly disclose vulnerabilities uncovered in their software. If export of security tools from the US were restricted, hundreds of thousands of vulnerabilities could go unpatched by companies until black-hat hackers exploit them maliciously. I urge the Department of Commerce to reconsider this proposal.

PUBLIC SUBMISSION

As of: 7/10/15 1:19 PM
Received: May 23, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j0j-647a
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0016

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael Ober

Address:

7679 Elmwood St
Roxborough, CO, 80125

Email: obermd@alum.mit.edu

Organization: Personal Comment

General Comment

We tried this already with encryption technologies during the 1990s. In the past six months two major security holes have been uncovered that are only applicable to those systems that still support the US Export Encryption rules from the 1990s. This is to say, almost every system on the internet is vulnerable as a legacy from our past laws.

While the US was restricting encryption technology exports other countries, including the very countries we were trying to prevent getting access to better encryption, developed their own computer security infrastructure, technology, and companies to the detriment to US.

Implementing this rule will have exactly the same effect and once again put US corporations at a competitive disadvantage relative to the rest of the world.

PUBLIC SUBMISSION

As of: 7/10/15 1:33 PM
Received: May 24, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j12-vfj1
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0017

Comment on FR Doc # 2015-11642

Submitter Information

Name: K Foster

Address:

CA,

General Comment

I am a cyber security professional involved in providing defensive cyber security measures. This means I use tools that detect vulnerabilities such as scanners and other tools as part of my job. I also provide penetration testing of critical systems using some of the tools you are proposing to restrict. Many of these tools are a collaborative effort and may include participate from other countries that may or may not participate in the Wassenaar Arrangement.

This is an example of regulation of materials by those who do not understand the impact and potential damage to both the industry and research sectors. Many system administrators use tools such as Kali, Cobalt Strike, and a whole host of Github projects to perform legitimate testing of the security of their networks. If these tools are treated as weapons with export restrictions this will result in several unintended consequences.

- First, all the developers of these tools will move off-shore which will result in a loss of talent and jobs.

- Secondly, independent researchers and other computer engineers and scientists will likely no longer perform the critical research needed to study, test, and detect security flaws under responsible disclosure.

- Finally, it won't stop malicious actors from using the tools.

From a cyber defense perspective, the same tools you propose restriction, thereby inhibiting future innovation, are the same tools American companies need to identify vulnerabilities and test their mitigations. This proposal actually reduces cyber security, not enhance it. I request you consider further comment, research and testimony by cyber security professionals in this industry.

PUBLIC SUBMISSION

As of: 7/10/15 1:35 PM
Received: May 24, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j13-xur9
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0018

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matthew Bergin

Address:

1016 Silver Oak Drive
Bakersfield, CA, 93312

Email: mbergin.infosec@gmail.com

Phone: 6613422140

Organization: The Vulnerability Mine, KoreLogic, Smash the Stack

General Comment

Entering this agreement will leave the United States in a position where furthering scientific research that would benefit the nation is not a priority. This agreement will discourage and potentially prevent researchers from leveraging their research in a commercially beneficial way. The taxonomy used in this agreement is highly generalized and overly broad. Should the United States enter into this agreement, many researchers will leave. As someone in the Information Security industry who has been considering leaving the United States as a result of the poor forethought put into Cyber Security legislation and trade agreements, I will be one of the ones leaving.

PUBLIC SUBMISSION

As of: 7/10/15 1:41 PM
Received: May 25, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j1w-5d32
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0019

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jon Lvy

Address:

P. O. Box 8588

NYC, NY, 10116

Email: xio@2600.nyc

General Comment

Data and networks do not have political, geographical, or ideological boundaries. Cyberwarfare does not stop at the border, and your data - this very submission, in fact - may travel through more countries than you can name while standing on one foot. No information technology (IT) specialist worth their salt would neglect the security of data nor ignore any source of information in helping him/her do so - whether that information originate domestically or from abroad.

This proposal's knock-on effect criminalizes the exchange of information which is vital and necessary for information technology staff to secure their data, determine if data has been breached, and informing the public so as to prevent further damage (be it in terms of dollars, euros, or invasions of privacy).

You cannot prevent cyberwarfare by merely not sharing; the information and tools are already out there. To assume so is akin to outlawing wooden sticks because of the off chance that someone might start a fire. For those of us in IT, that fire is what keeps our lighthouses shining brightly; the proposal as is, however, presumes all of IT to be arsonists.

This proposal is NOT in the public interest, this proposal in NOT in the private interest, this proposal is NOT in the interest of the United States, and this proposal in NOT in the interest of an interconnected planet.

PUBLIC SUBMISSION

As of: 7/10/15 1:42 PM
Received: May 25, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j20-9v16
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0020

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Williams

Address:

451 Sugarcreek dr
grovetown, GA, 30813

Email: malwarejake@gmail.com

Phone: 706-339-6713

Organization: Rendition Infosec

General Comment

The language of this document constitutes a gross misunderstanding of the technology surrounding vulnerability research. It is likely to create an environment where Wassenaar countries keep vulnerability technologies for their own use rather than working with vendors to patch discovered vulnerabilities.

Further, it is clear that if Wassenaar countries do not use the proposed changes to coerce researchers, then they will benefit from a dramatically reduced marketplace for vulnerabilities. There is almost nothing good that can come from creating a smaller marketplace for vulnerability researchers. This will largely criminalize security research in its current form. Simultaneously, it will likely increase the payments to vulnerability researchers who sell on the black market by reducing the number of legitimate outlets for vulnerability disclosure.

Finally, Wassenaar will make it difficult for firms to perform penetration testing across international borders. The vague language in Wassenaar proposals make it nearly impossible to determine which tools specifically can be brought across international borders.

If the Wassenaar countries are convinced that new rules are needed, then they must consult real technology experts - look to conferences like Blackhat, CCC, and others to find those working in the field to understand the ramifications. As much stock as governments tend to place in academics, doing so here is a clear mistake. You can only understand the ramifications of this proposal by talking to those in the field who are directly impacted by its adoption.

PUBLIC SUBMISSION

As of: 7/10/15 1:46 PM
Received: May 25, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j22-v7vf
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0021

Comment on FR Doc # 2015-11642

Submitter Information

Name: Scott Blaydes

General Comment

The Wassenaar Arrangement is a terrible idea. Computer security tools are not arms.

PUBLIC SUBMISSION

As of: 7/10/15 1:47 PM
Received: May 25, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j23-5nm0
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0022

Comment on FR Doc # 2015-11642

Submitter Information

Name: Clark Anonymous

Address:

UT,

General Comment

This is a very bad idea. The government cannot protect every company in the country. Without the ability to use these powerful tools to test and stress our networks, we will not be able to adequately protect ourselves. Taking away our ability to protect ourselves and our networks from threats both foreign and domestic is a infringement of our 4th amendment rights. I restate, this is a very, very bad idea.

PUBLIC SUBMISSION

As of: 7/10/15 1:49 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j24-7mwf
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0023

Comment on FR Doc # 2015-11642

Submitter Information

Name: Willard Dawson

Address:

GA,

General Comment

Others before me, and more to come afterwards, will have stated much more eloquently than I am capable how damaging this proposed agreement will be to software development and security research in particular. I cannot sit idly by while this misplaced effort as the WA currently stands in an attempt to improve security, as it clearly will have the opposite effect.

I am not optimistic that my comments nor those of others opposed to this agreement will be considered or acted upon, as it is my belief that the WA is the result of the lobbying of the defense industrial base, and not the good faith consideration of what is best for the participating countries economies or peoples. It is my hope that better senses will prevail, and that money and politics will be put aside just this once.

PUBLIC SUBMISSION

As of: 7/10/15 1:52 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2f-cnv5
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0024

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jonathan Zdziarski

Address: United States,

Email: jonathan@zdziarski.com

General Comment

I am a published and respected forensics expert who pioneered the very first forensic techniques to extract data from the iPhone as early as 2008.. Since then, I have spend several years, and much of my time, assisting numerous law enforcement and military agencies around the world, including our own. I've trained government agencies in the US, Canada, and UK, and trained law enforcement from dozens of our allies here at home in the US. My work has been validated by the NIJ/NIST. I have invested my time in providing free assistance to many US-based federal and state agencies who have flown personnel into my small town for help in the middle of the night. Because of my research and hard work, I've provided the necessary information to the rest of the industry to be able to perform iOS forensics, and a vast majority of today's forensics solutions are founded upon my techniques.

I did all of this on my own personal time, and in many cases on my own dime. The tools and techniques I have developed are by no means "intrusion" tools, however due to the excessively broad nature of the Wassenaar proposal, would fall under its regulations as they bypass security mechanisms of devices and collect information from them. As all of my research is done personally, I have no large company with lawyers to address the impossible spider web of export regulations that would be introduced by Wassenaar. The current proposal as is would harm far more than simply the information security industry, but would also greatly damage the forensics industry and ultimately limit the quality of tools available to law enforcement

agencies for conducting lawful forensics. My tools, as well as many commercial solutions, employ the use of exploits to collect information from devices for purposes that serve law enforcement and the greater good. I sometimes only privately release the source code to my own tools, as many commercial forensics manufacturers have stolen it in the past, yet I continue to help the law enforcement community. Wassenaar will do little to accomplish the goals it set out to, and instead make it impossible for security researchers like myself to further expand the base of knowledge by contributing openly to the community - which goes far beyond this country's borders.

Had Wassenaar been place in 2008, I would not have felt as though I could openly share my research publicly without risk of prosecution, which would have deprived the community as a whole - including the United States - of valuable information that has led to the greater good.

I understand there are certain nation states misusing intrusion tools to commit crimes. There are also many law enforcement agencies within the United States who have misused or abused my own tools and techniques to conduct questionable and potentially illegal intrusions. We cannot simply un-invent technologies to prevent their misuse, and unlike nuclear weapons, digital goods cannot be effectively regulated; yet this is the tradeoff we make, to create these tools for the greater good, knowing they may be abused. This proposal stands to only damage those looking to contribute to a better and more secure community. Wassenaar has a deterrent component, and at the heart of security research are many independent researchers like myself who will simply stop contributing if there is a fear of prosecution simply for sharing knowledge in the form of code.

Sharing knowledge is not only a basic human right, but the only means by which we can become a civilized society. Without knowledge and education, the greater good suffers. Security researchers share knowledge in the form of code, which serves as an illustration - a description - of a problem that exists in a system. Even many published papers will contain code as it is our language by which we can most effectively communicate an idea. In addition to code, binaries of it, to help test our own systems for vulnerabilities and ensure the security of our user base. Wassenaar, at its very core, attempts to regulate the ideas and knowledge we communicate through code. History shows that regulating knowledge on any level has proven detrimental to societies. In Wassenaar's attempt to prevent the dissemination of intrusion software, it is as the very core creating too much of a fear of prosecution to any security researcher to even consider developing or sharing their research with those who would most benefit from it.

There are alternatives to dealing with malicious nation states that do not involve putting regulations and the fear of prosecution on honest, law abiding researchers whose focus should be on their work, and not on being imprisoned by their own country. The day that I am prevented from sharing my knowledge freely with the world is also the day I stop sharing with all; it is the day the US declares they own the rights to my knowledge and what I do with it. That kind of power is far more dangerous than any intrusion tool.

PUBLIC SUBMISSION

As of: 7/10/15 1:53 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2i-wn2p
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0025

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

This threatens a lot more than basic rights. I have the right to exploit, manipulate, alter, modify, enhance, or otherwise change any portion of any product or device that I own. This includes hardware changes, software, changes, firmware changes, etc.

PUBLIC SUBMISSION

As of: 7/10/15 3:32 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2k-tehc
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0026

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Your boss

General Comment

This change will put companies in the United States at a distinct disadvantage when it comes to protecting user data, intellectual property, and trade secrets.

We need to keep the ability to research security issues, trade ideas, and tools to identify how the bad guys will come after us.

PUBLIC SUBMISSION

As of: 7/10/15 3:34 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2m-heqe
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0027

Comment on FR Doc # 2015-11642

Submitter Information

Name: Charlie Miller

Address: United States,

Email: cmiller@openrce.org

General Comment

I am an information security expert who has authored 3 books in computer security and given hundreds of talks at information security conferences. I have a Phd, have worked at the NSA, and am currently employed on the security team at Twitter. The proposed rule regarding exploitation licensing would outlaw almost everything I do and have done in my professional career. In its simplest form, I discover new vulnerabilities, new techniques to exploit systems, etc and then discuss this with the manufacturer in question, give talks and write papers about these vulnerabilities/techniques so that as a community, we can get better and improve the state of information security everywhere. Attackers will always continue to find new techniques and vulnerabilities and they are not hindered by laws which limit sharing. Only defenders will be penalized by limiting sharing of technical details of vulnerabilities and techniques. If, as a defender, I do not know what is the state of the art in attacks, I cannot defend against these attacks, or even properly distribute resources to try to defend my enterprise. Information security is not like physics or chemistry which is mostly static or at least very slowly changing. In just a few years, computer security changes radically as new software is created, new vulnerabilities produced, and new attack techniques invented. I hope that you will see that the field of information security is based on sharing information and that without this ability, we will not be able to defend our systems from attackers.

PUBLIC SUBMISSION

As of: 7/10/15 3:35 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2m-s1gr
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0028

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Software is not a weapon. Do not classify it as such.

If you want to regulate something, start with firearms, aka ACTUAL WEAPONS.

It seems trivial to try and regulate software, which kills NO ONE, yet actual weapons, used to kill thousands annually are more prevalent now than ever.

PUBLIC SUBMISSION

As of: 7/10/15 3:58 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2n-4m9t
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0029

Comment on FR Doc # 2015-11642

Submitter Information

Name: Bryan Owen

Address:

2347 Clubhouse Dr
Rocklin, CA, 95765

Email: bryan@osisoft.com

Phone: 360-957-5921

General Comment

Please register this comment in opposition to the proposed rule.

Details and ground of objection expressed are in full alignment with the attached position paper by Sergy Bratus PhD Dartmouth.

Furthermore, unintended impact may well degrade efforts to build more reliable software applications for use in critical national infrastructure.

Sincerely,
Bryan S. Owen PE
OSIsoft - Cyber Security Manager

Attachments

wassenaar-public-comment

Why Wassenaar Arrangement’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How To Fix It

Sergey Bratus, D J Capelis, Michael Locasto, Anna Shubina

October 9, 2014

Abstract

In this article we argue that Wassenaar Arrangement, as currently formulated, will have extensive harmful effects on computer security research and defensive software. We propose an alternative formulation that will achieve Wassenaar Arrangement’s goal of protecting activists and dissidents in oppressive regimes without causing these chilling effects.

1 The intent of the Wassenaar Arrangement

The Wassenaar Arrangement’s *intrusion software* clauses are intended to protect the activists and dissidents whose lives are endangered by government surveillance. The body of evidence that links persecution and computer surveillance is growing. The usual pattern of computing technology commoditization implies that this surveillance will grow in footprint and capacity while costs fall. The regulations of the Wassenaar Arrangement are intended to reverse or abate this trend, limiting the availability of computer surveillance to repressive regimes.

Unfortunately, as we demonstrate in this article, the Wassenaar definitions of *intrusion software* are overbroad, applying almost universally to elementary building blocks of security research. Among the unintended effects of the Arrangement’s definitions are chilling effects on the development of anti-surveillance measures and on the discovery of existing vulnerabilities—and thus on fixing vulnerable systems. The Arrangement’s definitions will impose a prior restraint on the publication of security research, analogous to the export controls on strong encryption software that were in effect in the 1990s.

The language of the Arrangement’s definitions attempts to avoid these unintended effects by using explicit exemptions as well as a two-tiered structure of controls. This article demonstrates that these methods fail to cover the majority of technological artifacts and processes that are crucial to security research and defense, and are therefore insufficient to meet the intent of the Arrangement.

The anti-surveillance intent of Wassenaar will, however, be fully fulfilled if surveillance-enabling software and hardware were to be addressed directly. We propose such a direct approach: targeting *exfiltration*, which is a key part of surveillance, rather than the vague and overbroad *intrusion*.

In addition to the advantage of simplicity, this approach eliminates the potential ambiguity between the singled-out but not directly controlled class of *intrusion software* and its related classes of *controlled items* in the current Wassenaar language.

This document has the following structure:

1. The conceptual structure of the chilling elements in the current Wassenaar language is discussed in section 2.
2. The overbreadth of these elements is discussed in section 3 and appendices A, B, and C.
3. Section 4 proposes replacing the key concept of *intrusion software* with *exfiltration software*. This proposed replacement addresses the Arrangement’s stated intent and avoids the unintended chilling effects.
4. The article concludes with a forward perspective on the regulation of independent security research, and an argument that such regulation must exercise caution in order to preserve the *citizens’ science* nature of such activity.

2 Definitions of intrusion software and controlled items in Wassenaar Arrangement

The Wassenaar Arrangement (WA) uses a two-step conceptual structure to define the surveillance-related software it purports to control. First, the WA introduces the concept of *intrusion software*, defined as

Software specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network capable device, and performing any of the following:

- a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or
- b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

The class of software defined by the previous quote is both broad and fundamental. As demonstrated later in this article, the class covers not only software known in computer security jargon as *exploits* and *rootkits*, but *all elementary means of software instrumentation, construction, and deconstruction* beyond the interfaces provided by the software’s pre-defined interfaces—despite explicitly excepting “hypervisors, debuggers or Software Reverse Engineering (SRE) tools” in the note to the above definition.

After defining intrusion software, the WA does not directly control this new class. Instead, the WA defines a *second*, controlled class of software and systems derived from the *intrusion software* class, namely those associated with *generation, operation or delivery of, or communication with*, intrusion software *and those for its development and production*.¹

The following elements are subjected to particular control:

4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, “intrusion software”.
4. D. 4. “Software” specially designed or modified for the generation, operation or delivery of, or communication with, “intrusion software”.
4. E. 1. c “Technology” for the “development” of “intrusion software”.
“Software” specially designed or modified for the “development” or “production” of equipment or “software” specified by 4.A. or 4.D.
“Technology” according to the General Technology Note, for the “development”, “production” or “use” of equipment or “software” specified by 4.A. or 4.D.

The apparent rationale for this two-step definition is that attempting to control elements of malware *per se* would inhibit communication between malware researchers and discovery of new vulnerabilities, a concern the authors of this article agree with. Controlling the second class, derived from the first, purports to limit the scope of the WA controls to the means of developing and delivering malware.² Unfortunately, this definition is still overbroad and will chill both basic and applied security research, as we explain below.

3 The problems with the Wassenaar Arrangement approach

Unfortunately, this two-class structure creates more problems than it solves. The so-called intrusion software class covers common and essential software techniques used throughout software engineering, not just potentially nefarious ones unique to malware and attack tools. In fact, these techniques are used by computer security products, remote management software, antivirus, enterprise reliability and monitoring, and operating systems.

Although this class of software is not directly controlled by WA, the software used to develop, generate, automate, and deploy it *is* controlled. This creates a huge potential for unintended consequences, since automation of development, analysis, and deployment is the primary way of making progress in software engineering, including but not limited to improving software reliability and security. Any non-nefarious software kinds and techniques deemed intrusion software under WA will have tools to improve their reliability and security controlled—and chilled.

¹Further details can be found in <http://dymaxion.org/essays/wa-items.html> by Eleanor Saitta. We would like to thank the author for helping us understand the WA’s structure of controls.

²We take this explanation from <https://www.privacyinternational.org/blog/export-controls-and-the-implications-for-security-research-tools#update>

The WA-defined intrusion software class is extremely broad. Centerpiece of the WA definition of intrusion software is “modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.” WA construes this behavior as a sign of nefarious intent, intrusion. However, such modification, is, in fact, *common and essential* for many software engineering techniques. Far from being unique to malware or to attack tools, the same techniques are used by remote management software, antivirus, enterprise reliability and monitoring, and operating systems. These techniques are to software engineering what saws, hammers, and planes are to carpentry; they are ubiquitous and indispensable.

Simply put, WA definition makes the mistake of equating techniques embodied in software with just *one* of its potential uses. This leads to a quagmire of unintended consequences.

Exceptions written into WA for this class do not help, because they exempt only a few kinds of tools among many kinds that are critical to security research and development. WA’s definition of intrusion software covers not only potentially nefarious software but also *all elementary means and techniques of software instrumentation, construction, and deconstruction* outside of the software’s own pre-defined interfaces. Since modern security software embodies complex combination of many techniques, a short list of exempted products will not be adequate to stop unintended consequences.

One strong unintended consequence will be complicating the development of defensive software techniques and products.

For example, the purpose of the popular *Detours* software library from Microsoft is to intercept and modify standard execution paths of software. Thus *Detours* squarely fits the WA’s definitions of *both* intrusion software and controlled items for developing such software. Yet *Detours* is a key industry tool for dynamic security patching of software, for monitoring software, and for debugging it. Many similar libraries exist for other operating systems and platforms, and others are currently being developed for new platforms such as smart phones.

As another example, the first personal firewall for Windows, the pioneering security product *Black-Ice*, installed itself by modifying the standard execution path of the Windows operating system. This technique made its installation easy, and contributed to the success of the product; it also allowed many users to secure their machines with the 3rd-party software when no solution from Microsoft was available. Outpacing vendor support is common for 3rd party software solutions.

In Appendix A we explain these technical cases in detail.

Controlling technologies of software development and automation is extremely broad and contrary to principles of software engineering. By starting with an overbroad definition of the *intrusion software*, the Wassenaar Arrangement subjects an even broader class of software tools to unwarranted control. Namely, WA’s control lists, as per items 4.A.5, 4.D.4, and 4.E.1, cover the automation of *development, generation, and operation* of software elements defined as intrusion software.

Yet automation is the primary means of software engineering and research. The absolute majority of modern software is *generated* with automation tools like compilers and linkers, which use development technologies such as templating and scripting. Modern software is also *operated* by means of automation tools. For example, the *Detours* library we mentioned above fits both definitions.

Moreover, the most promising modern Computer Science approach to analyzing vulnerabilities in software and to prioritizing them to be fixed by their potential input relies on techniques for Automatic Exploit Generation (AEG), which we cover in Appendix B. Yet all software tools and techniques involved would fall under the WA controls.

Keeping actual malware samples or exploit payloads off the controlled lists may seem like a way to allow security researchers and defensive software developers to communicate unimpeded. However, nowadays effective communication requires exchanging recipes, tools, and frameworks that *automate* finding of vulnerabilities and *generation* of exploits—exactly the items controlled by WA. Thus WA fails in its apparent intent to prevent chilling security research. We discuss this in detail in Appendix C.

Once we recognize that the class of software that forms the base of WA definitions is overbroad and must not be chilled for the sake of research and deepening our understanding of software flaws, then we must also recognize that the very means by which this understanding is advanced—automation of generation and operation—must likewise not be chilled.

We note that slowing or halting the progress of software engineering favors existing powers in the field, protecting them from the disruption of smaller private parties. This ultimately defeats the 3rd-party providers and the citizen’s science of security solutions to protect the dissidents and activists that WA seeks to protect.

4 Fixing Wassenaar: How to control surveillance without chilling security research

In this section, we outline our proposed approach to fixing the Wassenaar language, fully implementing its intent, and avoiding the chilling of computer security research.

Surveillance is exfiltration. Simply put, intrusive surveillance targeted by WA requires the surveilling party to receive sensitive data from the compromised computer. Without such receipt, surveillance cannot be said to have occurred. In nearly all of surveillance scenarios, surveillance software sends sensitive data to a command-and-control center operated by the government. The sending and the collection of sensitive data occur without the users' knowledge or permission. In other words, surveillance software critically depends on its ability to secretly *exfiltrate* data from the computer, without user permission or knowledge. Without this ability, surveillance effectively cannot exist.³

Exfiltration is thus key to surveillance. Controlling exfiltration functionality will therefore effectively control surveillance software. Hence we propose replacing the overbroad concept of *intrusion software* with *exfiltration software*, which we define as follows.

Exfiltration software is:

1) *Software designed to transmit data it did not create, or derived from data it did not create, except when any of the following conditions are met:*

a) *The creator of the data provides informed permission to the software to transmit the data.*

b) *A user or administrator of the computing system provides informed permission to the software to transmit the data.*

c) *Systems software set up by a user or administrator of the computing system provides the data to the software under the design of the computing system as part of routine and expected behavior.*

2) *Software designed to transmit data from the network in which it is contained to an external network, when installed or operated without direction of a user or administrator of that network.*

In the above definition, informed permission is permission explicitly given by a user or administrator through an interface that clearly communicates the intention and scope of the access, as well as all recipients of the transmitted data.

In the above definition, data includes but is not limited to messages, images, files, video and audio recordings, as well as data streams from the computer peripherals such as camera, microphone, and various sensors such as GPS, accelerometer, etc.

Since programs continually transmit data and create data, care must be taken that this definition is not overbroad like the definition of the *intrusion software*. In particular, this definition should not interfere with or burden legitimate advertising activities, legitimate software or hardware fingerprinting activities, and other legitimate data gathering activities. In the following sections, we show that these legitimate applications are not in danger.

4.1 E-commerce sites not in danger

E-commerce has long relied on *cookies* as a mechanism for maintaining web sessions. *Cookies* were introduced as early as 1994 in the Mosaic Netscape browser as a mechanism to support the concept of a session, that is to say, to allow the server-operating vendors to connect together all requests from the same web user, and to create the user experience of a continuous history of interactions, even though each web request was completed on its own and separately from others.⁴ Flash and HTML5 introduced

³The only remaining surveillance option would be to secretly accumulate surveillance data on the device itself, which is impractical for large amounts of data, prone to detection by the user, and requires physical retrieval of the user's device. Most importantly, this option fails to select targets out of the general population, which is the predominant use of surveillance by repressive regimes, and will remain so.

⁴From http://en.wikipedia.org/wiki/HTTP_cookie:

The term *cookie* was derived from *magic cookie*, which is the packet of data a program receives and sends again unchanged. Magic cookies were already used in computing when computer programmer Lou Montulli had the idea of using them in web communications in June 1994.[8] At the time, he was an employee of Netscape Communications, which was developing an e-commerce application for MCI. Vint Cerf and John Klensin represented MCI in technical

analogous mechanisms. These *cookie* and *local storage* data are created by the e-commerce vendor server software from the data transmitted to them by the client browser software.

The intent of these mechanisms is to maintain the identity of an e-commerce customer across a series of transactions between the customer and the e-commerce vendor, pursuant to the customer's intent of completing the e-commerce transaction, and to the customer's intent of maintaining a record of such transactions. Notably, the customer's identity tied to the payment method is explicitly provided to the vendor at customer sign-in time, since payment and disbursement of goods is only possible via a confirmation of customer identity.

Importantly, the decisions on what data to transmit and what data to store reside exclusively with the client-side software. Thus vendors of client software such as browsers bear the onus of protecting the users from inadvertently disclosing their protected private data. Indeed, these vendors responded to the user demands for protecting such data with introduction of such features as *private browsing* that explicitly disassociates users from the stored records of their previous transactions.

In summary, e-commerce software that acts within the scope of information explicitly provided by the users will not be chilled by the above controls.

4.2 Web ads not in danger

Web advertisement industry has long relied on collecting information pertaining to user visits to commercially operated websites, even though those visits have not resulted in an actual purchase—such as user searches for particular merchandise.

However, the data transmitted by the browser programs in the course of these visits is derived solely from the explicit user inputs, and from the program's inherent properties such as its version and supported communication formats, which are not protected private data according to the above definitions.

Thus targeted advertising based on user inputs is not chilled by the above controls.

4.3 Android, iPhone apps not in danger

Many applications of modern smart phones such as Android or iPhone depend on accessing potentially sensitive data such as the phone's location. However, both iPhone and Android apps request the user to explicitly approve their permissions to access such sensitive data throughout the app's lifetime. The user must grant these explicitly enumerated permissions before an app can install.

Thus development and profit models of Android and iPhone apps are explicitly exempt from the above controls.

4.4 Advanced browser fingerprinting not in danger

Recent research demonstrated that different versions of browsers implementing the HTML5 specification can be distinguished by how they process certain crafted drawing requests from the server.⁵ In particular, researchers from University of California, San Diego discovered that the differences in rendering of certain curves and patterns defined by the same mathematical formulas are enough for a server to distinguish between browser versions.⁶ Such research is important for preserving user privacy in the world of ever-increasing software complexity, since it anticipates how such complexity can be used or abused on the Internet.

However, all such observable differences stem entirely from computations performed by the browser programs themselves, without accessing any of the user-entered data whatsoever. Thus research into enumerating these differences will not be chilled.

discussions with Netscape Communications. Not wanting the MCI servers to have to retain partial transaction states led to MCI's request to Netscape to find a way to store that state in each user's computer. Cookies provided a solution to the problem of reliably implementing a virtual shopping cart.[9][10] Together with John Giannandrea, Montulli wrote the initial Netscape cookie specification the same year.

⁵“The Web never forgets: Persistent tracking mechanisms in the wild”, Acar et. al. <https://securehomes.esat.kuleuven.be/~gacar/persistent/>

⁶“Pixel Perfect: Fingerprinting Canvas in HTML5”, by Keaton Mowery and Hovav Shacham, <http://cseweb.ucsd.edu/~hovav/papers/ms12.html>

5 Protecting whistle-blowers

Whistle-blowers inform the public of abuses they encounter in the course of their employment by or business relation to the abusing organizations. To succeed, these whistle-blowers must provide credible evidence of abuses. Since the workflow of most organizations has by now been heavily computerized, there is a legitimate concern that abusers will use technological means as obstacles to whistle-blowing. Although so far the balance of power has favored the whistle-blowers, concerns remain that future technological developments will tip this balance. Consequently, software that might help whistle-blowers to expose evidence of abuses that they become privy to in the course of their business relationships should not be chilled.

We note that the proposed language preempts these concerns, since any data access in the course of a computerized business process is by definition approved by both the user and the owner of the involved computer device. While laws and contracts outside of the technology realms might govern disclosure of the data that is accessible to employees in the course of their employment, explicit access permissions must be set by administrators on behalf of employers, and are exercised and affirmed every time data is accessed.

Thus whistle-blowers are explicitly protected by the proposed definition.

6 Looking back to the 1990s “Crypto Wars”

The 1990s were a formative decade for the commercial Internet in the US. Unfortunately, during this same time the US government policy was to treat strong encryption as a threat and to control implementations of certain cryptographic algorithms as munitions, subject to vigorous enforcement of export regulations. In 1993 the author of the original PGP software, Phil Zimmerman became the target of an FBI investigation for munitions export without a license. This investigation lasted till 1996. At the same time a series of failed technological “solutions” and mandates, such as the backdoored-by-design Clipper chip⁷ and third-party key escrow were promoted as a legally safe way for telecommunications industry to implement compliant encryption—which would have essentially amounted to pretend security.

Export restrictions on artifacts of cryptography have doubtlessly harmed its practical progress. Not only Johnny Q. Public still can’t encrypt⁸, but John the Special Agent can’t encrypt either!⁹ No matter where one stands on whether and how much the latter should be allowed to wiretap the former, John certainly has things to hide and in fact a duty to hide them—in which he is conspicuously failing.

Could it be that *both* of these failures are due to the fact that deployment of strong cryptography was stymied just when today’s dominant communication protocols and infrastructure were rapidly developing? The fact is, they ended up leaving cryptography behind, and matured without incorporating cryptography at their core. Superiors of John the Special Agent may have had visions of him using separate, special technologies vastly stronger than Johnny Q. Public’s and obtained from sources untainted by the weaknesses of public commodity communications; it appears this vision was wishful thinking.

If having to pretend that poor cryptography was secure because practically exploring stronger cryptography was a legal minefield led us to this point, where would pretending that computers are secure because of a likely minefield arising in exploitation engineering lead us from here? It will likely be worse, because the field of cryptography by 1990s already had mature mathematical theory not easily undercut by the drag created on its engineering practice. Systems security, on the other hand, is only building up its theoretical foundations, and is in need of much more feedback and generalization of its practice.

If the practice of exploring the programming of programs’ faults becomes subject to regulation as vigorous as the so-called 1990s *Crypto Wars*, will this practice develop enough to warn us before unsecurable designs come to dominate in critical infrastructure, power management, medicine, or even household appliances beyond any hope of replacement? Will we be surrounded by an Internet of Untrustworthy Things just as we are surrounded today by an Internet of Things that Can’t Keep a Secret (or at least are no help to an ordinary person for doing so)?

⁷M. Blaze. “Protocol Failure in the Escrowed Encryption Standard.” Proceedings of Second ACM Conference on Computer and Communications Security, Fairfax, VA, November 1994

⁸www.usenix.org/events/sec99/full_papers/whitten/whitten.pdf

⁹http://www.usenix.org/event/sec11/tech/full_papers/Clark.pdf

7 Chilling of innovation, a long-term take

In a long-term perspective, all innovative software is *intrusion software*, inasmuch as it relies on unforeseen composition. Composition is what people do with software from its inception to application; it defines all interesting systems. All unforeseen, unexpected, or unapproved composition—otherwise known as innovation—is “intrusion” in WA terms.

In the classic realms of expressive works—copyrighted texts, music, and other arts— *Fair use* is unapproved compositional intrusion on pre-existing material, and one of the fundamental exceptions to requiring prior approval. The realm of systems engineering needs a protection equally strong to evolve.

Engineers and researchers being liable for creating “intrusive” tools branded as violating copyright is seen as a chilling effect on innovation. Similarly, engineers and researchers working on techniques painted as intrusive should enjoy similar protections, for similar reasons. Construction of “intrusive” unapproved mash-ups should be no crime, but an ordinary and protected means of gainful employment (being, as it were, an engineering discipline right on the innovation trajectory).

The nature of engineering is creative reuse and pushing the limits, unexpected applications of existing products (not just ideas). Unapproved composition is at the heart of innovation.

Innovation is unapproved composition. In software, we know it as *exploitation*. In software, any composition for which dedicated interfaces were not foreseen, pre-designed, envisioned, or provided is *exploitation*. It’s impossible for a designer to foresee all uses of a technology, or most productive uses, or even the primary use a decade from now – who could have predicted the WWW when designing multiuser machines? Inventors of the telephone envisioned its profit model as receiving information services from a central office, not as overwhelmingly a means of private conversations. When a monopoly manages to enforce an envisioned set of uses for an extended period, stagnation results.

In the case of security and privacy, stagnation at the current point would mean the status quo of ubiquitous insecurity and institutionalized imbalance of power between the state and the citizens, between well-funded attack and resource-constrained defense.

Even though a Hollywood view of exploitation is that of enabling cinematic attacks, exploitation enables defense by orders of magnitude stronger.

A Why the WA intrusion software definition has wrong granularity that exceptions cannot fix

The WA defines *intrusion software*, and thus by derivation also *controlled items* for *generation, operation or delivery of, or communication with or development of intrusion software*, in terms of fundamental operations of computer science research and software engineering. Generally speaking, the operations in the definition are as fundamental as operations such as taking roots, proof-by-contradiction, or variable substitution are to mathematics. These operations are present in all non-trivial, innovative software (see Section 7). These operations are critical to the performance of state-of-the-art security research, as well as to other kinds of technological progress in software engineering. These operations are especially critical for improving defense. At the same time, the exceptions to these definitions (“Hypervisors, debuggers or Software Reverse Engineering (SRE) tools; ...”) are at a different, much higher level than *whole programs* or products built for a particular purpose.

Complex software is built in multiple levels of aggregation and composition. Innovation entails aggregation and composition in unforeseen combinations, at many levels. The WA definitions whitelist a particular set of combinations and compositions that are seen as important to software engineering *today*, but does not and cannot include the set of all such combinations and compositions that will become equally or more important in the future.

The excepted programs or products contain both components with functionality labeled *intrusive* as well other kinds of components. For example, a debugger contains software for *modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions*—such as a module that injects breakpoints to divert control of the debugged program or device—and a GUI. Without a GUI, the breakpointing software component could be considered “intrusion software”; a reasonable judge who had even practiced debugging with an integrated production debugger may be swayed by the argument that software that lacks a GUI is *not* a debugger and thus not excepted.

Yet it is in these execution-modifying (or *execution-hijacking*) components that progress in debugging tools, in observability, and in security of software, is made. For example, Microsoft’s release of its Detours library was a significant step forward. As described by Microsoft, Detours is both *intrusion software* and a *controlled item* by the language of the Wassenaar Arrangement.

Detours intercepts Win32 functions by re-writing the in-memory code for target functions. The Detours package also contains utilities to attach arbitrary DLLs and data segments (called payloads) to any Win32 binary. —<http://research.microsoft.com/en-us/projects/detours/>

Detours can be used as a component of a debugger or as a part of malware. For example,

Malware authors like Detours, too, and they use the Detours library to perform import table modification [standard technique of diverting standard execution paths into new code/commands supplied by a Detours user], attach DLLs to existing program files, and add function hooks to running processes.

Malware authors most commonly use Detours to add new DLLs [containing their malicious code/commands] to existing binaries on disk. [discussion of various malware authors’ techniques follows]

— *Practical Malware Analysis*, Michael Sikorski and Andrew Honig, No Starch Press, 2012, page 262, Chapter 12.

Detours implements the pattern of modifying the execution path of other programs known as *hooking*. Hooking is a basic pattern that is used ubiquitously for all kinds of software composition. Hooking is used for debugging, instrumentation, and performance tuning of software. Hooking is also used for patching vulnerabilities in software, as well as to upgrade software that lacks a dedicated upgrade mechanism. This latter function is a critical security function for legacy software, including the software that runs critical physical infrastructure.

Moreover, Detours is popular with developers, because

the Detours library makes it possible for a developer to make application modifications simply.

—Ibid.

The hooking pattern implements the fundamental software engineering operation of *composing* software with other software. For this reason, it is implemented by a great variety of software, with a wide range of techniques and uses. Often the hooking software is developed and released separately; sometimes it is released together with management tools and automation tools.

Detours also includes a *management* component for its means of modifying the execution path, and for *automating* the actions that deploy these means. These components fit the WA definition of controlled items, since they operate, manage, and automate the application of the means by which Detours modifies the execution path.

A.1 “Standard execution path” contradicts the nature of modern software design

WA language depends on the concept of the *standard execution path* of a piece of software. The implication is that for every piece of software or at least for most important kinds, a set execution path exists, and modifications of it are suspect and likely onerous.

However, modern software engineering in fact emphasizes customization of software, which explicitly modifies the standard, as-shipped execution paths! For example, the popular Firefox web browser includes a mechanism for modifying most aspects of its functionality (that is, its execution path) with the so-called Add-ons, which interleave *externally provided instructions* with the main Firefox code logic. Over ten thousands of Firefox add-ons are available at the time of this writing from the official Firefox vendor site alone. Similarly, Google’s featured browser, Chrome, includes an analogous mechanism.

Software customization mechanisms for modifying the *standard execution path* of the software that forms the basis of the Internet as we know it are not limited to web browsers. For example, the Apache web server that, according to Netcraft web surveys, is the leading software behind roughly 40% of all Internet web sites, ships with a similar customization mechanism.

In fact, the ability to modify the standard execution path of programs is the basis of an entire new programming paradigm, Aspect-Oriented Programming. Popular programming languages such as Ruby and its Ruby-on-Rails leading web development environment, implement this paradigm in the form of *mix-ins*, a standard language mechanism.

Thus the WA emphasis on *standard execution path* is misleading, and clashes with the trends of modern software engineering. One way to reconcile this language with these trends is to assume that *standard* in fact has the much narrower meaning of *expected by developers*. We make this assumption in the following analysis.

A.2 Bypassing protective countermeasures.

Wassenaar language targets “defeat[ing] protective countermeasures”, explained in a footnote as “techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) or sandboxing.” But what does *defeating* mean? This language appears to include any software composition (such as patching or jailbreaking) that work reliably on systems with a *protective countermeasure* enabled.

ASLR. For example, the point of ASLR is to make the location of various software components when loaded into the memory of a computer less predictable. To patch such software while it’s running (such patching is known as *hot-patching*, used for servers and other devices, including mission-critical devices that are expected to operate 24/7), the patching software typically scans the computer’s memory and identifies the addresses (locations) that were *randomized*.

This memory scanning technique is one of the most fundamental research and engineering operations. Software that performs this non-trivial operation and looks for patterns in memory can be developed and distributed on its own, or with other components such as pattern-matchers for memory contents or memory visualizers. In any case, it can be said to *defeat* ASLR, by making available to its operator the information obscured by ASLR; a reasonable judge familiar with technology would find this statement true at face value.

For example, the F.L.I.R.T. technology is used by IDA Pro, a reverse engineering tool to locate library functions, which are obscured by ASLR. F.L.I.R.T. is identified by the tool’s maker as a separate technology.¹⁰ Since its publication, other software based on the same principles and dedicated to the task of scanning memory at runtime has been developed by various parties and has aided in a variety of applications such as forensics and hot-patching.

The operation of scanning memory to locate specific software components is too fundamental and low-level to ascribe to it any intent or any specific use; yet it “defeats” the obfuscation imposed by ASLR by definition.

¹⁰https://www.hex-rays.com/products/ida/tech/flirt/in_depth.shtml

Sandboxing. Sandboxing is a key engineering practice of limiting a program or a device in its access to system resources. However, since the engineering practice is so generic and ubiquitously used, bypassing the restrictions of a sandbox is also frequently used.

For example, *jailbreaking* of mobile phones to bypass manufacturer restrictions “defeats” sandboxing. To make it easy for non-technical users to *jailbreak* and *unlock* their iPhones, developers of the jailbreak delivered the jailbreaking commands through a browser exploit (altering the execution path of the browser software); the user merely had to navigate to a webpage to get the jailbreak take effect (delivered).

All of these activities, including those allowing users to customize and protect their phones, would be chilled by WA language.

“Defeating protective countermeasures” is not a meaningful way to characterize software. Protective countermeasures are no different from any other obstacles to exploitation; it does not matter in the final security analysis whether, e.g., the attacker cannot control the computation flow because the memory corruption afforded by a bug is serendipitously not extensive enough or because a protective measure somehow captures the attempt. In either case, security analysis deals with a system of constraints; it doesn’t matter where constraints come from, or even whether they are external or internal to the target system. Separating these constraints by origins would merely confuse and weaken development of rigorous analysis.

Moreover, the intent to bypass countermeasures is neither obvious nor easy to argue. A piece of malware—or a defensive 3rd party security product like the pioneering BlackIce product described below—may use a specific method of altering the target software either because that method is more reliable or because the original vendor blocks some simpler methods. Intruding equals composing in every technical sense.

A very good discussion of this topic can be found in Rob Graham’s story of how he built the first personal firewall BlackIce: <http://blog.erratasec.com/2013/03/the-debate-over-evil-code.html> Rob was able to inject his protective code (in WA terms, “intrude”) on the Windows operating system manually, but today a similar composition effort to harden, say, an iPhone, would notably require automation, which would fall into controlled lists of WA.

B Automated Exploit Generation

WA control lists specifically target *generation* and *development of intrusion software*. Thus they apply directly to generation of exploits, which are means of modifying the execution path of software.

Automatic generation of exploits is a rapidly developing direction of security research. The promise of this field is to identify and prioritize security-critical software bugs so that they can be eliminated. Prioritization is important, because modern complex software contains a multitude of bugs, many of which are not exploitable; demonstrating that a bug is exploitable generates the exploit, which scientifically and incontrovertibly proves this fact. In the words of the leading academic group that coined the term AEG,

The generated exploits unambiguously demonstrate a bug is security-critical. Successful AEG solutions provide concrete, actionable information to help developers decide which bugs to fix first.

Although the name *Automatic Exploit Generation* (AEG) does not suggest it, AEG is in fact a task closely connected with *software verification*, a research and engineering methodology that uses formal methods to secure software. Continuing the above quote:

Our research team and others cast AEG as a program-verification task but with a twist [...]. Traditional verification takes a program and a specification of safety as inputs and verifies the program satisfies the safety specification. The twist is we replace typical safety properties with an “exploitability” property, and the “verification” process becomes one of finding a program path where the exploitability property holds. Casting AEG in a verification framework ensures AEG techniques are based on a *firm theoretic foundation*. The verification-based approach guarantees sound analysis, and automatically generating an exploit provides proof that the reported bug is security-critical.

—*Automatic Exploit Generation*, by Thanassis Avgerinos, Sang Kil Cha, Alexandre Rebert, Edward J. Schwartz, Maverick Woo, and David Brumley, Communications of the ACM, February 2014, Vol. 57, No. 2, p. 74

In a nutshell, AEG is a promising method of containing vulnerabilities that is based on firm theoretic foundation of proven computer science.

As with fuzzers, development of industry-strength AEG engines starts with prototypes built by individual researchers or academic groups, but then moves to commercial startups to accommodate the scalability, performance, and other engineering challenges that require dedicated effort of professional developers. Yet this is also the stage in which such research produces its most fundamental results and proves its ability to handle real-world software. Chilling AEG would severely set back defense.

C Why WA control items will impede progress of software security

We referred earlier to the apparent rationale for the WA language not controlling so-called exploits or rootkits, but instead controlling the software that is used to *generate* or *operate* or *deliver* exploits, and to develop all the above.

Several points must be made about this language:

1. It presents fundamental obstacles to engineering progress of security tools, and to vulnerability research in particular.
2. Its practical application to actual research and engineering artifacts used in vulnerability research is just as vague as that of *intrusion software* or potentially even more vague.

This language presumes a clear boundary between programs that implement a particular software functionality and the programs used to create such implementations. In reality, no such clear boundary exists.

The structure of classifying software and the way that software progresses is misconstrued in the underlying concepts of the supposed dichotomy. *In fact, all of our technical examples above easily fall into the controlled category of intrusion software enablers!*

Progress in software engineering is being made by abstracting functionality from products first into libraries and then into domain-specific languages and development tools. Early computers took a single program (modern low-end microcontrollers still do), later computers required a specialized program to *operate* other programs; this program is now known as an *operating system*. Early programs were written in the basic commands of the computer, and realized basic conceptual elements of programming such as loops and conditionals in these basic commands; later programs were written directly in terms of these conceptual elements, and required specialized programs to *generate* the actual basic commands or to emulate them. These specialized generating programs became respectively known as compilers, interpreters. A middle ground was taken up by *virtual machine* (VM) programs, such that run automatically generated hybrid *bytecode* commands for Java and .Net programs and at the same time *operate* them.¹¹

Thus parts of functionality continually move from *programs* to the *libraries* (which standardize both operation and programming) and the *tools*, and specifically by way of tools incorporating the functionality to automatically generate what used to be manually written code in the main program's body.

Without this migration of logic from programs to *development tools*, without thus abstracting away the complexity, progress in programs is impossible. But under WA logic, this migration would create controlled items even if the programs themselves are not controlled. Thus *abstraction*, the key means of deepening our understanding of both engineering and research issues, will be chilled.

When does code for some functionality stop being a part of an uncontrolled program and becomes a controlled *tool*? Does this happen when it moves to a library? A shared library? A piece of environment that must be present for the main program to operate? When it moves into a tool to be generated automatically from an abbreviated instruction or statement or code line in the program?

Moreover, not every code that is automatically generated is generated by a compiler. It may be generated by several levels of scripts from templates, by a *Makefile*, or a scripted build, by any part of the build system, and so on. Present day's build systems are complex and multi-layered, and each layer creates automatically generated code. There are no clear boundaries where code templates end and *generated* code begins.

It is only thanks to this progression of automating operation and generation of programs that we were able to advance from relatively small and simple programs to the present state of software engineering and research.

¹¹Such are the Java VMs inside web browsers and inside Android phones.

Security research follows the general pattern of software engineering. There is broad recognition among security researchers that the better, more principled kind of defenses that common operating systems employ now, commercially known as DEP, ASLR, EMET, and others are a result of *co-evolution* of offensive research and defensive systems research.

Advancement of vulnerability research, key to this co-evolution, required substantial engineering investment—into exactly the kind of generation and operation aspects of offensive software. In full accord with the general trend described above, so-called exploits and rootkits went from entirely hand-coded for the occasion to use of libraries, then to specialized compilers, build systems, interpreters, and remote proxying designs comparable with production virtual machines emulators.

For example, initial defenses against the Return-Oriented Programming techniques (so known since the academic publications of 2007-8, but known to vulnerability researchers since at least 1999-2000) did not take into account the fact that finding of the snippets of code in the target that were composed by the attacker to program the target without introducing any binary code could be automated. While it was clear to security researchers experienced in offense that automation was possible and likely, and also that a skilled attacker would need far less than complete automation to bypass existing defenses, the threat was not so clear to vendors.

It took building actual *ROP compilers* software to perform these tasks automatically and in a platform-independent manner to present the defenders with a proper yardstick for testing their actual and proposed system defenses. Yet ROP compilers clearly fall among the WA controlled items.

Fuzzers: a highly practical approach to discovering vulnerabilities, threatened. A necessary requirement for software to be considered trustworthy is that the software operates predictably and as expected no matter what inputs it receives. This requirement is especially important when the software receives inputs that can be maliciously crafted by attackers (which is, e.g., the case for any software that receives its inputs from the Internet). Unfortunately, software engineering and development practices are not yet at the point when this requirement can be assured.

As a result, an effective method of discovering security vulnerabilities in current software is to supply that software with a series of crafted, invalid inputs and to observe which inputs cause unexpected effects such as crashes or modifications of the typical execution paths. Such inputs are referred to as *fuzzed* inputs by security practitioners, and the process of generating these inputs and observing their effects is referred to as *fuzzing*. The software that automates this process is called a *fuzzer* or a *fuzzing framework*.

Fuzzing is by now the subject of several industry textbooks,¹² a large number of research papers, and an integral part of the secure software development lifecycle. Major vendors of software and hardware such as Microsoft and Cisco use fuzzing in their software development and testing processes.

However, fuzzers and fuzzing frameworks fall within the WA definition of the controlled items, because they automate a crucial step in development of *intrusion software*: finding the potential points where the *standard execution path* of the target software can be modified, and logic external to the target program purpose can be introduced.

Until new emerging methodologies for engineering input-handling code become a universally accepted industry standard, fuzzing will remain a key technique for software security testing. Controlling the development of new fuzzing techniques and of software that implements them will set back the existing industry practices by years if not decades.

Vulnerability-finding tools must generate “intrusions” to be effective. To fulfill their business purpose, vulnerability-finding tools such as fuzzers must generate *complete* recipes and payloads for “modification of the standard execution path” that would put a target program or process under attacker’s control. Stopping short of producing and testing such recipes would hinder a necessary business function of the tool: prioritizing vulnerabilities into those actually exploitable under constraints imposed by defensive measures such as DEP and ASLR, and those not exploitable. To effectively allocate the inherently limited specialist labor to fixing the actually exploitable vulnerabilities first, a vendor must receive evidence of exploitability. Since bugs in complex software systems are plentiful, following this evidence-based approach is a virtual necessity for software vendors.

Moreover, the ability of fuzzers and other automated security tools to find vulnerabilities depends on their ability to exercise all code paths possible in the target software, *including those not normally exercised*. In other words, this ability depends on finding precisely those execution paths that an *intrusion*

¹²E.g., “Fuzzing: Brute Force Vulnerability Discovery”, by Michael Sutton, Adam Greene, Pedram Amini, Addison-Wesley Professional, 2007; “Fuzzing for Software Security Testing and Quality Assurance”, Ari Takanen, Jared DeMott, Charlie Miller, Artech House, 2008.

software would use. A fuzzer is essentially a tool for automatically generating recipes for triggering these paths.

Consequently, vulnerability analysis tools developed towards algorithmically automating security analysis and striving to automate judging of a bug's exploitability. Modern research tools such as EXE¹³ and KLEE¹⁴ use sophisticated static and dynamic automated analysis methods; similar proprietary techniques are used in industry by Microsoft and other major vendors.

Can a fuzzer avoid being controlled by stopping short of producing a complete intrusion or exploit? Only at the cost of ignoring state-of-the-art research. Early fuzzers indeed stopped at producing recipes for triggering bugs that led to crashes, and left the rest of the exploitability analysis to costly manual analysis by experts. As a result, these early fuzzers tended to produce more leads than defenders could investigate, nor provided defenders with any actionable prioritization between the triggered bugs. Such levels of performance is currently neither acceptable nor scalable, with few exceptions.

Automating operation and generation of code is the only way of making progress.

Operational automation and generation of code by tools is how software engineering makes progress. They enable us to write larger programs, but that is less than half of the story—they also enable us to see what actual challenges and possibilities come to the forefront when we reach each level of scale and complexity.

It used to be that the job of system administrators was to manually enter commands to operate systems in their care. Automation of these commands in common operational scenarios was what made Cloud Computing possible (while dropping costs of hardware made it economically feasible in its present form). Automation is at the core of every engineering advance; in computing, it is generation of logical commands or code that gets primarily automated.

Law that creates obstacles to automating operation and generation of software—any software—impedes the key means by which computing progresses. If the class of software that is broad—as *intrusion software* as currently defined is, being essentially unapproved composition—then restricting automation of operation and generation of this kind of software is going to catch all the practical ways to make engineering progress in this software.

Essentially, such restrictions seeks to freeze the evolution and understanding of the so-called *intrusion software* in its present state. This will create gaps in understanding and ability between actors who can afford the chill and those who cannot, such as private parties, small companies, startups, and small groups of research, and individual researchers.

In summary, the current Wassenaar approach will fail to protect both security researchers and the basic conditions for progress in security engineering.

¹³“EXE: automatically generating inputs of death”, Cristian Cadar, Vijay Ganesh, Peter M. Pawlowski, David L. Dill, and Dawson R. Engler, 2006, In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA

¹⁴“KLEE: unassisted and automatic generation of high-coverage tests for complex systems programs”, Cristian Cadar, Daniel Dunbar, and Dawson Engler, 2008, In Proceedings of the 8th USENIX conference on Operating systems design and implementation (OSDI'08). USENIX Association, Berkeley, CA, USA

PUBLIC SUBMISSION

As of: 7/10/15 3:59 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2n-tan9
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0030

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Hello,

As an information security professional, I can say with confidence that passing this modified arrangement will be detrimental to personal information and security across the globe.

By restricting vulnerability management, detection, encryption, and other similar tools, you put those who are most at risk in most harm. In the field of information security, sharing and collaboration is what makes everything more secure, and one of the pillars of what makes it function.

As much as I do not like the sale of exploits and vulnerabilities, I feel that this does much more harm than good. I am totally against companies like VUPEN and FinFisher being able to operate with essential impunity, but with that said, many of the speech included in this will restrict technology used to protect dissidents in other countries, and those that are living under regimes with oppressive internet policies. Countries like Tunisia, Syria, and Libya all had thousands of refugees, and many of them were able to travel and communicate safely using technology developed in the United States.

Please, scrap this ammendment. Take it back to the drawing board. I understand that many are afraid of what the new cyber world will hold, but please, do not restrict code in this way, it will do more harm than good.

Thank you for your consideration.

PUBLIC SUBMISSION

As of: 7/10/15 4:02 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2o-2t14
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0031

Comment on FR Doc # 2015-11642

Submitter Information

Name: leo gomez

General Comment

It has never been a problem. Why make it one now. Keep it legal.

PUBLIC SUBMISSION

As of: 7/10/15 4:03 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2p-q7y6
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0032

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jasper Rogers

General Comment

Keep jailbreaking legal!

PUBLIC SUBMISSION

As of: 7/10/15 4:05 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2q-x2z9
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0033

Comment on FR Doc # 2015-11642

Submitter Information

Name: Gregory Hetrick

General Comment

The addition of exploits to the Wassenaar arrangement is an egregious mistake for anyone that cares about a more secure and less surveilled Internet. The negative knock-on effects of the agreement include, but are not limited to, the following list:

1. It provides governments with a massive coercive tool to control public security research and disadvantage non-military security research. This coercive power need not be exercised in order to chill public research and vulnerability disclosure.
2. It tilts the incentive structure strongly in favor of providing all exploits to your host government, and makes disclosure or collaborative research across national boundaries risky
3. It provides a way to prohibit security researchers from disseminating attack tools uncovered on compromised machines.
4. It risks fragmenting, balkanizing, and ultimately militarizing the currently existing public security research community.

In short additions would cause a less secure internet not a more secure by stifling legal security research.

Intrusion Software should not be included in the Arrangement.

PUBLIC SUBMISSION

As of: 7/10/15 4:06 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2q-3kde
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0034

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Are you fucking kidding me? This is WAY overreaching! STOP, ALREADY, and instead do good for a change.

PUBLIC SUBMISSION

As of: 7/10/15 4:08 PM Received: May 26, 2015 Status: Posted Posted: June 18, 2015 Tracking No. 1jz-8j2q-9sqs Comments Due: July 20, 2015 Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0035

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Just a few comments and or thoughts, your proposed rule has literally just raised many and some very interesting ideas.

People that I am acquainted to, work for security protocols daily, and they themselves find this very ignorant

Reason being, they modify their personal computers, cars and mobile phones to their liking. They do this cause of security issues they them selves find from the original seller! So they make it secure for them selves

I myself have a jail broken iPhone, I use this phone for work as well, and before jailbreaking my phone I noticed my phone acting slow at times, seems odd for a brand new iPhone 6+

That a side when I jail broke it I installed a privacy third party app/tweak

And it let me know when the microphone was trying to be accessed, low and behold it brought it up multiple times WHILE I was not using my phone

That is a security breach for my company, and I don't want to loose my job/personal things to some company that can get away with it, while I pay for MY DEVICE, just like any computer I buy I want to install my own software for preferences

That all aside, why can I install a custom software into my car stereo, my home computer, laptop but not my mobile phone!?

This is a very fine line everybody is walking on and I'm glad that I live in United States, where the rich can get away with everything, just to make more money to give to the government.

PUBLIC SUBMISSION

As of: 7/10/15 4:09 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2q-myeb
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0036

Comment on FR Doc # 2015-11642

Submitter Information

Name: Tyler Nighswander

Address:

1102 South Abel St

Apt 443

Milpitas, CA, 95035

Email: tylerni7@gmail.com

Phone: 203-441-0022

General Comment

Please see the attached document, as my comments were slightly over the limit allowed by this form.

In summary, as a security researcher, I strongly oppose the proposed rule, and urge you to do the same.

Attachments

comments

BIS-2015-0011-0001 (Wassenaar) is a terrible idea. The only effect this legislation will have on cyber security is to harm legitimate researchers, and thereby make illegal activities even easier for cyber criminals.

First off, what problem is Wassenaar trying to address? Computer security has been a growing problem for the past decade, and it seems its importance has been growing at an exponential rate. There are reports in the media every week of large scale intrusions on companies and government organizations. Presumably the goal of Wassenaar is to attempt to stop or at least slow down these sorts of cyber attacks. However, it is not clear at all how Wassenaar will accomplish this. Will Wassenaar affect nation-state actors who are responsible for many of the breaches in the media? Clearly not; rogue nation-states are not going to be punished under our laws. In that case, this must help to prosecute criminals who use computers to attack corporations or people. However, what they are doing is obviously already illegal, and they clearly don't care. So it would seem this legislation will not help on that front.

Supporters of Wassenaar might view things differently. Perhaps their view is that limiting "tools of the trade" will hinder cyber criminals. Although obviously not perfectly successful, ideas such as this have been used for physical weapons in the past, so why not apply them to "cyber weapons"? The problem with this is that physical materials and weapons are much less versatile and far easier to keep track of. It's conceivable that a shipment of AK-47s could be caught at a border by customs or other agents; unfortunately there is no analogous way to keep track of digital tools that computer criminals may use. Further, physical munitions are easier to classify than digital tools. You can't do much with high-capacity magazines besides put them in guns--but so called "intrusion software" can be used by forensic investigators, malware researchers, penetration testers, and computer security educators for very legitimate uses. So what would the effects be of limiting "intrusion software"? Well, criminals will easily exfiltrate tools undetected over the internet (or in publications, or through hand carried memory cards, etc), as there is no possible way to stop them. Meanwhile legitimate researchers who wish to obey the letter of the law will be shut down and unable to protect the internet.

We can ignore the impossibility of actually controlling the exportation of "intrusion technologies" and examine what would happen to malicious actors if we were able to limit the proliferation of these technologies. Ignoring the fact that legitimate researchers are now hindered from doing their jobs to stop criminals, what impacts will criminals feel? It could be the case that certain public tools might now be difficult for criminals to access which could hamper their attacks. However, these tools are discussed in thousands of published papers, books, patents, and articles on the internet and in print. So even if it might be the case that certain pieces of software will not be available online or for purchase, nothing prevents criminal organizations or nation-states from producing more. And again, as there are no physical supplies required short of computers, there is no way to stop the creation of new tools by malicious actors.

Legislators obviously don't intend for Wassenaar to only disrupt the activities of legitimate researchers, but that is exactly what they will do. As countries have accepted "intrusion software" into their definition of dual-use technologies, security researchers have already begun to feel the

impact. A couple examples are [1], a tool published online for malware and forensics analysts that was removed after German law made the tools illegal; and [2], a yearly contest in which companies such as Google and Microsoft pay researchers for "intrusion software" into their own products so that they can improve their security, has recently had trouble with researchers participating in countries where their activities may be considered illegal. As a computer security researcher, it's frightening to think about how much more difficult my job will be as other researchers stop releasing tools or information for fear of breaking the law.

Despite what anyone says, making "intrusion software" illegal or requiring an arms license is clearly already harming researchers. Currently America is one of a dwindling number of places where computer security innovation prospers and remains free. It is foolish to think that changing this will do anything but harm for our nation's security.

Although the Wassenaar does provide for the ability to get licenses in order for researchers to continue work, this is not an acceptable compromise. Independent researchers or those who cannot afford or are even rejected for licenses will be shut down; and in a community with an already high sense of paranoia, filling out an application for intent to research "cyber munitions" would be an impossibly high barrier to entry. Despite the provision for licenses, the results will stay the same: numerous legitimate and beneficial security research will halt.

One reaction to all this would be to go back and try to improve the definition of "intrusion software". However, this is a futile approach. There is no way to specifically target software used for evil versus that which is used for good. The entirety of the Anti-Virus industry is built on attempting to solve a problem even easier than this, and they still have not found an acceptable solution. Instead, we should take a step back and work to create laws that address the real issue: illegal cyber activities. Most states don't regulate lock-picks, but do regulate burglary or breaking and entering; so too should it be for computer security. Leave the tools available to those who wish to use them for good, and punish criminals who use them for illegal purposes.

As it stands, including "intrusion software" into Wassenaar actually fails on three of the four criteria that Wassenaar itself uses to add new items to the list of dual-use technologies [3]: these technologies are available globally to anyone with a computer, controlling the exportation of computer software is impossible, and creating clear and objective specifications for software used for malicious purposes is a problem known to computer scientists to be provably impossible [4].

Although I can sympathize with legislators' desires to curb the computer security problems facing the world, it is painfully obvious that these rules will do more harm than good. They harm researchers whose goal is to secure software as well as researchers who work to track down computer criminals; meanwhile actual criminals are completely untouched and can continue to operate unmolested.

If you value this nation's security, I urge you to do everything you can to prevent the proposed BIS-2015-0011-0001.

(For more technical descriptions on how "intrusion software" can be used for securing systems, [5]

is an excellent article and provides a handful of concrete examples.)

[1] <http://www.trapkit.de/research/sslkeyfinder/>

[2] <http://www.net-security.org/secworld.php?id=17961>

[3] http://www.wassenaar.org/controllists/2005/Criteria_as_updated_at_the_December_2005_PLM.pdf

[4] http://en.wikipedia.org/wiki/Halting_problem

[5] <https://www.usenix.org/system/files/login/articles/wassenaar.pdf>

PUBLIC SUBMISSION

As of: 7/10/15 4:11 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2q-rf4u
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0037

Comment on FR Doc # 2015-11642

Submitter Information

Name: Lucas Elmer

General Comment

do not make jailbreak illegal they do nothing wrong...

PUBLIC SUBMISSION

As of: 7/10/15 4:11 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2q-d068
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0038

Comment on FR Doc # 2015-11642

Submitter Information

Name: Rory McDonald

General Comment

People should be able to use their devices how they want...they own it, it is up them how they want to use it. It's not illegal to modify a car, lawnmower, etc., why would this be any different?

PUBLIC SUBMISSION

As of: 7/10/15 4:12 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2r-vbkb
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0039

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

bruh make dat jailbreak legal!!!!

PUBLIC SUBMISSION

As of: 7/10/15 4:12 PM
Received: May 26, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2r-boyp
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0040

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

There is no reason it should be illegal to jailbreak your phone. You are simply using your device that you paid for to the fullest extent.

PUBLIC SUBMISSION

As of: 7/10/15 4:13 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2u-bk3a
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0041

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jake Anonymous

General Comment

Jailbreaking and device modification allows for invention. America was built on tinkerers and those who dove deep to determine how something worked, Samuel Slater's textile technology being an example. He reverse-engineered and modified textile machinery bringing America into the industrial age. Let Americans tinker. Let them learn. Let them discover. Let us grow.

PUBLIC SUBMISSION

As of: 7/10/15 4:14 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2u-1yj7
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0042

Comment on FR Doc # 2015-11642

Submitter Information

Name: John Labelle

Address:

432 West Wilson St

#2

Madison, 53703

Email: argentage@gmail.com

Phone: 6088526661

General Comment

It's basically unimaginable that this would deter the people it is intending to deter. There is no notion of a centralized industrial production process for software security, and so no reasonable path to locate and prosecute parties who don't wish to comply. It will hinder companies who voluntarily comply and never, ever stop anyone who is intending deliberately to circumvent the law (because there are innumerable ways to get said data outside of the country.)

I don't understand why anyone would think this was a good idea.

PUBLIC SUBMISSION

As of: 7/10/15 4:14 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2u-mogo
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0043

Comment on FR Doc # 2015-11642

Submitter Information

Name: Kerem Ylmaz

General Comment

I bought my own device, and I think I should be free to do whatever I want on it unless I don't block someone else's freedom. Jailbreaking Apple devices should NOT be illegal.

PUBLIC SUBMISSION

As of: 7/10/15 4:15 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2v-7f58
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0044

Comment on FR Doc # 2015-11642

Submitter Information

Name: Luca C

General Comment

Jailbreak is not a crime

PUBLIC SUBMISSION

As of: 7/10/15 4:16 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j2z-5lgo
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0045

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

This is a very dumb bill. Considering. Not only will they be able to eavesdrop, but using alternate ways of avoiding/blocking this such as jailbreaking an iphone, will become illegal! Its our government at its finest... Being stupid as hell!

PUBLIC SUBMISSION

As of: 7/10/15 4:17 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j34-t8dp
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0046

Comment on FR Doc # 2015-11642

Submitter Information

Name: Logan Browne

Address:

17990 Crother Hills Rd
Meadow Vista, CA, 95722

Email: logan@rosetrace.com

Phone: 9166553980

General Comment

I have worked in computer security for over 20 years, and have extensive experience analyzing and understanding computer code that is used for exploitation and remote surveillance.

This type of computer code is not something that can be easily identified or controlled, even by experts. There are so many ways that it may be implemented, and detection of all the ways to attack programs is not mathematically possible.

The proposed regulation of the sale of security vulnerabilities and computer code creates a regulation that would be tremendously expensive for the government agency tasked with enforcement and which would not be effective in averting the risks.

PUBLIC SUBMISSION

As of: 7/10/15 4:17 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j34-59yb
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0047

Comment on FR Doc # 2015-11642

Submitter Information

Name: Joseph Leavitt

General Comment

Extending the reach of the Wassenaar Arrangement to include Intrusion and Surveillance Items will have a negative effect on the security posture of U.S. companies and have no positive effect on curbing malicious activity. Please do whatever it takes to prevent this change. Thank you.

PUBLIC SUBMISSION

As of: 7/10/15 4:18 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j35-oh8z
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0048

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

MAKE JAILBREAKING LEGAL! IF YOU OWN A SMARTPHONE, YOU DESERVE TO HAVE ADMIN RIGHTS TO IT!

PUBLIC SUBMISSION

As of: 7/10/15 4:18 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j3a-md3c
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0049

Comment on FR Doc # 2015-11642

Submitter Information

Name: B. Calvin Saul

General Comment

Should this be implemented, only criminals would have the ability to test their own software for vulnerabilities.

PUBLIC SUBMISSION

As of: 7/10/15 4:19 PM
Received: May 27, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j3d-4lsv
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0050

Comment on FR Doc # 2015-11642

Submitter Information

Name: Joseph Autry

Address:

200 Paddington Ct

Alpharetta, GA, 30009

Email: tim.autry@gmail.com

General Comment

I hope the government(s) realize that clamping down on pen testing, white hat hacking or looking for 0-day exploits is only going to cause the web to be less secure.

The reason is, you are making it against the law for them to do their job, so they can find these issues before the black hats do and make use of them.

Labeling a program or process in the cyber world is not as easy as saying yes this is bad outlaw it or now this is good allow it. The same program or process can be used by the good guys or the bad guys it is just a difference in what the person using it is trying to do.

White hats, pen testers and 0-day researchers are attempting to find these problems before the black hats do and report it to the software, hardware or firmware manufacturer, giving the vendor the time to patch the problems.

On the other hand the black hats, they are just the opposite, and using the same software the White hats use, the only difference is when they find a problem, they use it to penetrate a company's network and/or sell it to the highest bidder, sometimes its the NSA, other times it

maybe China or Russia, I'm not really sure how that part is handled, but they spread bad proof of concept or actually working code to the public, no controls, no oversight and before the vendor can research and create a fix/patch, the black hats have already stolen millions of dollars worth of money, or data, data that can be used to get more money or data from corporations, like directly do a debit from a company's bank account to some offshore untraceable bank account, done several times over so the traceable information gets lost on the internet put the money ends up in various bank accounts for any number of uses, drugs, sex trade, pirating other software, buying other exploits, or buying personal data from legitimate companies to put with personal data they either bought and/or stolen portraying other people - aka - identity theft.

Please if you must continue in this direction, have plenty of white hat hackers, legit pen testers and coders on hand to discuss this with. I don't mean the CIOs, IT Directors or Managers, I mean the guy/gal that comes in and works trying to hack a company's website, or pen test a company's network, or writes code to fix 0-day exploits. They legitimately get paid by the company they are hacking, pen testing or coding for to do this. To find the weakness or exploit before the black (bad) hats do.

Thank you for your time and any consideration you may take with my suggestions.

PUBLIC SUBMISSION

As of: 7/10/15 4:20 PM
Received: May 28, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j3v-hjbe
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0051

Comment on FR Doc # 2015-11642

Submitter Information

Name: Karim HadjSalem

Address:

81 Cheney Ln

East Hartford, 06118

Email: karim113@yahoo.com

Phone: 8605505215

General Comment

Given that there's no effective way to determine constructive versus destructive software, and there's no implication of being able to in the Agreement, this is a short-sighted attempt to fix a problem that the drafters have no concept about. A good example is PEN testing software versus some blackhat toolkit that is used nefariously.

PUBLIC SUBMISSION

As of: 7/10/15 4:21 PM
Received: May 28, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j3v-b9fc
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0052

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matt Linton

General Comment

To whom it may concern;

I am writing today to express my disapproval and disappointment at the addition of language into the Wassenaar agreement which would prohibit the transfer of computer software "for intrusions".

I am a cyber security professional in the private industry, charged with protecting the private data of over a billion individuals who have a vested interest in being safeguarded from unauthorized access to their data. The tools which I use daily to keep these users safe include tools which under the vague definitions in the proposed bill would be potentially made criminal.

As my team is international and needs to share tools with one another to do our jobs, these export restrictions would damage our users and harm our ability to keep our systems safe.

Additionally I have concerns that, as with typical corporate responses to the ITAR law, companies and their legal departments may resort to overly-broad internal interpretations of this law and prohibit even more collaboration than the authors intend to prohibit. The propensity for corporate legal departments to "be safe" rather than risking a lawsuit or legal charges is real and would further reduce my ability to protect my company and its users.

Please stop trying to regulate the tools of my trade.

Respectfully,
Matt Linton
Incident Response & Forensics Specialist

PUBLIC SUBMISSION

As of: 7/10/15 4:21 PM
Received: May 28, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j3x-1qho
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0053

Comment on FR Doc # 2015-11642

Submitter Information

Name: Stephen Marney

Address:

5319 Bangor Dr

Kensington, 20895

Email: stephen_marney@techsyn.com

Phone: 202-570-0327

General Comment

Any prohibition of cybersecurity research is unwarranted and ill advised. Merely identifying any such research as a topic for possible control will have the effect of diminishing this valuable research.

Also any use of consumer- or business-oriented cryptography should be uncontrolled. Encryption is a human right as the UN recently clarified.

PUBLIC SUBMISSION

As of: 7/10/15 4:42 PM
Received: May 29, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j45-pkue
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0054

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

don't let this happen

PUBLIC SUBMISSION

As of: 7/10/15 4:29 PM
Received: May 29, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j48-30ow
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0055

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

Organization: Planet Zuda, LLC

General Comment

Security research is vital to making sites more secure, sadly this proposal will make things much harder for researchers and security companies. What BIS forgot when writing this proposal is that the ethical security researchers have clients who want them to make proof of concepts. A proof of concept is proving that the zero day can be exploited. If this arrangement prohibits that, then then will undermine the security of U.S companies and abroad.

Many companies run automated tools to check for certain known vulnerabilities, so they can patch them. This implementation appears that it will make that much harder, if possible at all. This will make companies and the U.S government a lot more insecure. Those who want to commit crimes will still commit crimes, while those who want to stop people from committing crimes with security holes will be slowed down or prohibited to do so, because whoever wrote this implementation didn't understand security research.

We hope this won't be implemented, but if it is this will affect countries that aren't even part of this arrangement, because companies they used to hire to help secure their service will now be under a misguided attempt of legislation.

PUBLIC SUBMISSION

As of: 7/10/15 4:28 PM
Received: May 29, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j4e-qft1
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0056

Comment on FR Doc # 2015-11642

Submitter Information

Name: Alex Green

Address:

Westminster, CO,

Email: alexgreen00@gmail.com

General Comment

You are encroaching on our free speech, weakening cyber security, and you will not be able to keep up with those that you are trying restrict.

PUBLIC SUBMISSION

As of: 7/10/15 4:29 PM
Received: May 30, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j52-6mu4
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0057

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

The proposed changes put forward for comment need to be prevented from implementation in their current form.

These changes will raise the risk for security researchers, cyber threat/vulnerability assessors, and penetration testers all professions vital to the future security and safety of Americans who use and conduct business over the internet, and even using a computer off-line.

While the proposed changes would apply to the security professionals (white hats) and the cybercriminals and their organizations (black hats) equally in theory, the proposal overlooks a fundamental truth of law; by definition, criminals do not obey the law.

Security research would be drastically affected, as the risk to the legitimate people and organizations trying to help keep Americans safe while using their computers would rapidly increase to the point that it outweighed the return for these professionals. Meanwhile, the criminals would continue to do business as usual, for breaking one more law would make no difference to their bottom lines.

The result of the implementation of these proposed changes would be an overall decrease in the safety and security of IT systems across the board in this country for consumers and businesses, as the security researchers would no longer be devoting as much collective energy to finding and publishing the hidden vulnerabilities the criminals are using to exploit and misappropriate

the systems they target. Without the published warning, the criminals would still have the same access and capabilities our consumers and businesses would simply be unable to protect themselves as well, as they would no longer be advised of the threat, and unaware of what measures would need to be taken to increase their security posture and reduce their threat exposure.

PUBLIC SUBMISSION

As of: 7/10/15 4:29 PM
Received: May 30, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8j52-6mu4
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0057

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

The proposed changes put forward for comment need to be prevented from implementation in their current form.

These changes will raise the risk for security researchers, cyber threat/vulnerability assessors, and penetration testers all professions vital to the future security and safety of Americans who use and conduct business over the internet, and even using a computer off-line.

While the proposed changes would apply to the security professionals (white hats) and the cybercriminals and their organizations (black hats) equally in theory, the proposal overlooks a fundamental truth of law; by definition, criminals do not obey the law.

Security research would be drastically affected, as the risk to the legitimate people and organizations trying to help keep Americans safe while using their computers would rapidly increase to the point that it outweighed the return for these professionals. Meanwhile, the criminals would continue to do business as usual, for breaking one more law would make no difference to their bottom lines.

The result of the implementation of these proposed changes would be an overall decrease in the safety and security of IT systems across the board in this country for consumers and businesses, as the security researchers would no longer be devoting as much collective energy to finding and publishing the hidden vulnerabilities the criminals are using to exploit and misappropriate

the systems they target. Without the published warning, the criminals would still have the same access and capabilities our consumers and businesses would simply be unable to protect themselves as well, as they would no longer be advised of the threat, and unaware of what measures would need to be taken to increase their security posture and reduce their threat exposure.

PUBLIC SUBMISSION

As of: 7/10/15 4:30 PM
Received: June 07, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jap-lao9
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0058

Comment on FR Doc # 2015-11642

Submitter Information

Name: Rick Howard

Address: United States,

Email: rahhoward@gmail.com

General Comment

So why am I opposed to these new rules? I have two reasons; one large and one small. The large reason is that implementing these controls will not solve the problem. I understand what they are trying to do; keep cyber attack tool sets out of the hands of bad people and bad states. But these cybersecurity items are not the same kinds of arms that have been successfully controlled by the Wassenaar Arrangement in the past. Dual use technologies -- like centrifuge devices used in the creation of both nuclear bombs and nuclear power rely on advanced hardware manufacturing processes that consumed buckets of R&D money, took years to develop and is the intellectual property of a small set of manufacturers. Exporting that technology to states that do not already have the capability to build it themselves without keeping track of it would be irresponsible. Software attack tools, on the other hand, can literally be built by anybody who has a laptop, a compiler and a mindset that is keen to understand how things work and how one might subvert an original design for other purposes. They do not have to start from scratch either. The basic designs of Stuxnet, Flame and DuQu are readily available on the Internet. It would not take much for a small team of modestly resourced hackers to build their own. Buying exploits to feed your attack platform would not be hard either. The underground economy for exploits has been around since the Internet was a collection of tin cans and string. These new export rules will not affect that in the least.

By implementing the 2013 Wassenaar Arrangement rules, the only thing you accomplish is

making it harder for legitimate commercial organizations to sell their products and services abroad. In other words, if one of the Defense Industrial Based companies wanted to sell their internally developed attack platform to Iran, the Wassenaar Arrangement members would know. I guess that is something but it puts a burden on these companies without coming close to accomplishing the goal: prevent bad actors from getting attack platforms.

My smaller reason is that these new rules create a chilling affect on the white hat security research community. It is hard to know the exact numbers, but I estimate that the volume of vulnerabilities discovered by independent white hat researchers compared to the original development company responsible for all of the software that we like to run is quite high. These new Wassenaar Arrangement rules will dampen the enthusiasm of white hat researchers pursuing responsible disclosure and bug bounty programs.

For both of those reasons, I do not see why the Department of Commerce would enforce these rules.

PUBLIC SUBMISSION

As of: 7/10/15 3:52 PM Received: June 09, 2015 Status: Posted Posted: June 18, 2015 Tracking No. 1jz-8jbq-vzbb Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0059

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jason Syversen

Address:

Siege Technologies
 540 North Commercial Street
 Manchester, NH, 03101

Email: info@siegetechnologies.com

Phone: 603-747-9800

General Comment

To whom it may concern,

The proposed intrusion and surveillance items rules are, simply put, a disaster. It is hard to even determine what ill the proposed regulations are supposed to be addressing.

I was a researcher for ten years, program manager at DARPA managing cyber security R&D and now run a multi-million dollar cyber security R&D firm with ~20 employees. I've worked in the past with senior personnel in the USG to develop/clarify classification rules (also a challenge.) A key takeaway in that process was that defining terms, and grouping technologies in offense/defense is hard and should only be undertaken cautiously. Sometimes nothing is better. One "offensive tool" is another's defensive technology. Someone's "novel approach" is another party's legacy capability.

The strategic problems with the document are the lack of clarity over intended restrictions, the obvious challenge of enveloping intrusion software but not the software itself, the ambiguous

definitions of the intended products, and the ripple effects of restricting cyber security research, development, and testing software will have on the broader security research community.

In the newly released FAQ it states the intrusion restriction is NOT covering malware, but would "control the command and delivery platforms for generating, operating, delivering, and communicating with "intrusion software". It would also control the technology for developing "intrusion software," but it does not control the "intrusion software" itself." How exactly would a researcher do one but not the other? If traveling to another country with the research on your machine you are searched you could be found a criminal exporting technology because you have some test code for analyzing malware! Or a program to take over the C2 (command and control channel) for a botnet to bring it down/analyze it. How does one define the delivery of intrusion software? They are bits, traveling over a wire or wireless connection via a protocol like TCP/IP. Is the network card involved in the delivery? Or perhaps the wire itself is now an export item? Or is it really the command line where the "send" command was typed, that's the key? I assume none of these are intended to be included, but the audience considered needs to be a technically ignorant judge and/or jury potentially involved in a dispute and the track record there is uninspiring.

And the surveillance equipment restrictions are even more broad and vague. "Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor" I assume that the BIS does not intend these to include tools like Wireshark and normal software but is attempting to curtail tools used to suppress dissidents or monitor citizens whole sale in other countries, but it is impossible (certainly with the current language) to make that distinction.

Criminalizing research is an extremely dangerous and harmful approach that will set back computer security potentially a decade or more. Criminal groups, terrorists, foreign nations will continue unabated but legitimate research organizations, academics, and individuals in the United States will significantly restrict or curtail their research (and certainly their public presentation) of anything associated with C2 (see: operating/delivering), hacking (see, generating), fuzzers or debuggers (see developing). Several months ago, Exelis corporation wouldn't let me into a building to discuss a new cyber security project because I didn't have a passport with me out of fear of violating export control. The ripple effects of export regulations are far reaching and usually unintended.

These proposed rules will affect nearly every research program we have going on. From software protection to software security test software, to security networking research, to finding ways to find/remove vulnerabilities, to software agent design, to moving target defense (which includes testing against attacks,) everything we do will put us in danger of fines and jail. As a result we will restrict some work that we will take on, reduce who we hire or partner with (dual citizen employees count as export violations, hiring experts is already our biggest challenge), reduce/eliminate our publications and contributions to public research, and spend significantly more on lawyers. Some employees may choose careers at Google or others to avoid liability. (We lost a key employee to Samsung because of similar frustration with USG security procedures.) The significant cost we incur will not enhance US/world security at all.

Please remove this language all together. If is deemed that something must be implemented despite the significant collateral damage, please cautiously engage a large group of domain

experts_.

Sincerely,

Jason Syversen
CEO, Siege Technologies

PUBLIC SUBMISSION

As of: 7/10/15 4:35 PM
Received: June 11, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jd1-pvob
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0060

Comment on FR Doc # 2015-11642

Submitter Information

Name: John Berry

Address:

966 Mud Pond Road
Thetford Center, 05075

Email: john.n.berry@gmail.com

Phone: 4104126523

General Comment

I am a computer security professional who deals with these types of products on a daily basis. I am also an active member in the Capture The Flag community where we design software to purposefully have 0-days. This aids in the advancement of research and the skill sets of the hacker community at large. Passing these rules would be devastating to both of these communities. Attacking systems with 0-days is the entire purpose of CTF and by making these controlled items we would no longer be able to do this. Our community would be destroyed overnight.

This proposed rule seems to have been written by people who do not actually have a firm grasp of the words they are using.

PUBLIC SUBMISSION

As of: 7/10/15 4:36 PM
Received: June 11, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jd5-99sj
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0061

Comment on FR Doc # 2015-11642

Submitter Information

Name: John Bryk

Address:

6725 Greenleaf St.

Springfield, VA, 22150

Email: jbryk@dngisac.com

Phone: 7038629466

Organization: DNG-ISAC

General Comment

Submitted on behalf of the Downstream Natural Gas ISAC

John Bryk

DNG-ISAC Analyst

The proposed BIS rules go beyond the simpler Wassenaar rules, affecting a large number of cybersecurity products, and cybersecurity research. These rules further restrict anything that may be used to develop a cyberweapon, which therefore make a wide number of innocuous product export-restricted, such as editors and compilers.

One of the major dangers of imposing export controls on surveillance systems is the risk of overreach. While you want the scope of the systems being controlled and the language to be wide enough to catch the targeted product and its variants, you also need the language to be specific and detailed enough to ensure that no items get inadvertently caught at the same time.

Good and evil products are often indistinguishable from each other.

That means things like bug bounties that encourage people to find 0-days in your software, so that you can fix them before hackers (or the NSA) exploit them, will be controlled. That means scanning tools that hunt for any exploitable conditions in your computers, to find those bugs before hackers do, will no longer be available without expensive licensing and government oversight. Companies, including DNG members, use surveillance tools on their own networks (like intrusion prevention systems) to monitor activity and find hackers.

Wasenaar targets evil products but they inadvertently catch the bulk of defensive products in their rules as well. I would suggest targeted enforcement against bad actors as opposed to a sweeping, revenue-raising, government control program.

PUBLIC SUBMISSION

As of: 7/10/15 4:37 PM
Received: June 15, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jfu-h8y6
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0062

Comment on FR Doc # 2015-11642

Submitter Information

Name: Avindra Goolcharan

Address:

1 Ackerman Ave
Clifton, NJ, 07011

Email: aavindraa@gmail.com

Phone: 973 289 1042

Organization: N / A

General Comment

This is an absurd proposal. It is ambiguous and infringes upon the basic freedoms of both people and enterprises.

I am not going to speak at length about why this is so problematic, but I will add my voice to the (hopefully, a sea) of complaints.

PUBLIC SUBMISSION

As of: 7/10/15 4:37 PM
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh1-rc44
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0063

Comment on FR Doc # 2015-11642

Submitter Information

Name: Gregory Conti

Email: gjconti@rumint.org

Organization: Private Citizen

General Comment

While the Wassenaar Arrangement is well intentioned, it is an overly broad and dangerous policy that will have a dramatic chilling effect on legitimate vulnerability research, security audits, and independent security research in general.

Vulnerability research holds companies publicly accountable for the security of their products and plays an important role in securing the nation, not just in terms of critical infrastructure, but also in the millions of consumer products that are hastily rushed to market and security is an afterthought to be bolted on later, if at all.

Think electronic voting. Independent security researchers identified myriad vulnerabilities in voting machines that embarrassed manufactures by highlighting the flaws in their products, despite hyped marketing claims to the otherwise. Without this work, insecure electronic voting machines would be in widespread use and threatening the foundations of our democracy. Similarly, independent researchers studied the security of automobiles and demonstrated that manufacturer claims of robust security were patently wrong. As a result, automobile manufacturers are starting to take security seriously and are creating research labs focused specifically on securing their products.

These are just two of many examples of positive change that would not have occurred if

independent vulnerability research was made effectively illegal as part of the Wassenaar Arrangement.

The future Internet of Things, where billions of day-to-day items will be networked and residing in our homes, workplaces, automobiles, and on/inside our persons, is primed and ready to be a security catastrophe. (Consider the recently announced, wi-fi enabled interactive Barbie, with Siri-like artificial intelligence that we place in the hands of our children, or the smart-phone enabled garage door opener available at home improvement stores for \$248, both are security incidents waiting to happen). We need to empower the independent security research community to identify the flaws in these and other products to help maximize security while unlocking the potential societal benefits these products offer.

Security vulnerability research also plays a critical role in cyber defense. Both commercial and open source vulnerability assessment tools rely on databases of known vulnerabilities and allow network defenders to legitimately perform due diligence testing of the networks under their charge. The vast majority of the vulnerabilities in these tools have been responsibly disclosed and protect us against known threats. While not perfect, such tools represent a best practice that at least provides a baseline of security. In some cases, inclusion of a new vulnerability into a vulnerability assessment tool is the only means to incentivize a manufacturer who has been dragging their feet to implement a solution.

Today the independent security vulnerability community identifies and responsibly discloses a stream of vulnerabilities that would otherwise be unknown in public forums and unlikely to be fixed by manufacturers as there is no business case to do so. This significant work output of vulnerability researchers secures our infrastructure and the global commons of the Internet. Many companies have partnered with the vulnerability research community by offering highly regarded bug bounty programs.

It is also important to remember, that effectively criminalizing vulnerability research wont stop criminal actors, just stop the critical, necessary, and law abiding work being done above ground. The flaws will still exist, we just wont know about them, companies wont be incentivized to fix the ones that are known, and ultimately we will all be far less secure.

Perhaps the most disturbing aspect of the Wassenaar Arrangement is the chilling effect it will have on all security researchers. Now more than ever we need to unlock the full potential of the security community rather than criminalize it. My voice is one among many and Ive only covered a few key points. I encourage you to listen carefully to the responses from others in the security community, now more than ever we need their help.

I am making these comments as a private citizen. The views expressed are my own and do not reflect the official policy or position of West Point, the Department of the Army, the Department of Defense, or the US Government.

PUBLIC SUBMISSION

As of: 7/10/15 4:38 PM
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-qivs
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0064

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Malware sandboxes are containers specially designed to communicate with intrusion software. By running captured intrusion software in a sandbox and communicating with it, sandboxes allow for deeper analysis of malware and the gathering of threat indicators. Malware sandboxes occur in the Fireeye defensive appliance, most antivirus engines, mwcollect, the Cuckoo Sandbox, and a litany of defensive software projects. Due to the fact that they are specially designed to communicate with intrusion software, malware sandboxes are controlled as a Class 2 item. Please confirm (y/n)?

<http://directory.fsf.org/wiki/Mwcollect>

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-dk04
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0065

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, 20151

Email: mikef@kududyn.com

Phone: 703-527-1230

General Comment

Information Sharing and Threat Intelligence software is specially designed to develop effective malware sandboxes (regulated as "Any software or system specially designed to generate, operate, deliver, or communicate with intrusion software"). By providing Threat Indicators to malware sandboxes (such as malware decryption keys, command and control sequences, etc.), these special design features allow for the distributed gathering and sharing of threat intelligence. As Information Sharing software and Threat Intelligence software is specifically designed to develop a controlled item, they are controlled items. Please confirm (y/n)?

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-9kad
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0066

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Many tools are required for the development of intrusion software; a complete list would greatly exceed the time constraints available. A partial list of required software is listed below; the guidance grants an exception to some of this software (marked as **). All other software on the below list would be controlled as technology required for the development of intrusion software (marked as \$\$).

1> Compilers \$\$.

2> IDE environments \$\$.

3> Programming languages \$\$.

4> Debuggers **.

5> Software Reverse Engineering tools (SRE) **.

6> Virtualization test environments \$\$.

7> Data flow tracking tools with virtualization support \$\$.

8> Emulators \$\$.

9> Hypervisors **.

10> Code editors \$\$.

11> Operating Systems \$\$.

Please confirm that tools that the tools above that are required for the development of intrusion software including compilers and operating systems are controlled: (y/n)?

PUBLIC SUBMISSION

As of: July 10, 2015 Received: June 17, 2015 Status: Posted Posted: June 18, 2015 Tracking No. 1jz-8jh7-1w6r Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0067

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

General Comment

The definition of intrusion software includes any software which modifies the standard execution path of a program or process in order to allow the execution of externally provided instructions. It must be noted that a special exploitation technique, Return Oriented Programming (ROP), is able to achieve tasks without externally providing instructions and as a result does not meet the WA definition of intrusion software. While software which modifies or extracts user or system data is intrusion software, any computing task accomplished by a ROP exploit which does not modify or extract user or system data does not qualify as intrusion software, including:

- the computation of crypto currencies such as bitcoin
- the extraction or modification of crypto keys not kept as system data, including those stored off board in hardware or a TPM
- cyber-physical destruction
- the direct acquisition of sensor data
- modification of off-system compute resources such as hard disk firmware etc.

We appreciate that the FAQ notes that exploits that result in cyber-physical destruction are not

controlled; please confirm that all ROP exploits which perform a task which does not modify system or user data (per the above) are also not controlled: (y/n)?

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-93x8
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0068

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

The Wassenaar Arrangement (WA) defines intrusion software as a small subset of known exploit techniques and other software. This subset fails to include numerous exploitation techniques including side-channel timing attacks, resource consumption attacks, ROP, etc. This subset also includes a number of techniques that are not exploitation (such as auto-updaters). Notably, aside from this language, WA does not include any restrictions on rootkits or malware; the BIS language similarly does not attempt to define rootkits or malware. Rootkits are kernel-level data-hiding tools; malware is any software unwanted by the user.

- a) Please confirm that rootkits and malware are not included in any proposed BIS control: (y/n)?
- b) Please confirm that BIS has not attempted to define rootkits or malware (y/n)?

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-m7p1
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0069

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Many companies such as Google, Facebook, and Microsoft operate contests to improve their software defenses. In these contests, zero-day exploits are delivered, demonstrated, collected and awarded prizes. The result of these competitions is new mitigations against entire categories of software attack. Notably this month HP and Google were awarded a cash prize from Microsoft for the creation and delivery of a zero-day exploit:
<http://googleprojectzero.blogspot.com/2015/06/dude-wheres-my-heap.html>
<https://technet.microsoft.com/en-US/security/dn425049>

These contests award prizes to intrusion software; contestants must use tools that generate, operate, and communicate with intrusion software while contest organizers must operate competition frameworks that deliver intrusion software.

Please confirm that both the operating frameworks (Microsoft) of these contests and the delivery software used by their participants (Google) are controlled (y/n)?

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-lbm4
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0070

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Both cybersecurity competitions [2] and security training courses use intentionally vulnerable test software with weak protection mechanisms to test the skill of competitors and evaluate students. This software is fake and only fielded in controlled test environments and sandboxes. An example is the Hacksys Extreme Vulnerable Driver, a system component filled with many known security mistakes used for educational purposes [1]. These intentionally vulnerable software samples (challenges) are operated on test systems for training purposes and do not guard the privacy or data of any person. Training material and contest participant submissions defeat the intentionally weak protections and deliver instructions or modify data, making them intrusion software. Thus, cybersecurity competitions and training courses must communicate with, generate, and deliver intrusion software. Please confirm that cybersecurity competitions and training frameworks are controlled (y/n)?

[1] <http://www.payatu.com/hacksys-extreme-vulnerable-driver/>

[2] <http://www.theguardian.com/technology/2014/jan/30/top-uk-hackers-compete-cybersecurity-challenge-gchq>

PUBLIC SUBMISSION

As of: July 10, 2015 Received: June 17, 2015 Status: Posted Posted: June 18, 2015 Tracking No. 1jz-8jh7-cg9i Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0071

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Many security firms publish zero-day exploits in malware. For instance, Cisco recently released a zero-day exploit in the Teslacrypt ransomware[1], which allows users to defeat the protections of the computer running Teslacrypt, extract the decryption key, and recover their files. Zero-day exploits in malware which defeat the intended execution path of malware include virus/rootkit uninstallers, ransomware key recovery tools, and other such softwares. Note that in practice, exploits against rootkits and other intrusion software are used to defend the Internet [2]. These tools are classic exploits and meet every checklist item in the intrusion software definition; as a result, any software that is specially designed to generate, operate, deliver, or communicate with these tools is controlled. This includes most adware removal suites, networked ransomware remediation, and some forms of antivirus which allow web-only operation.

Please confirm that all of the above classes of software are controlled (y/n).

Note: The BIS FAQ indicates that anti-virus software is not controlled, however anti-virus software contains zero-day exploits that attack malware; these specific antivirus components are

clearly controlled, hence the above (carefully scoped) question.

[1] <http://blogs.cisco.com/security/talos/teslacrypt>

[2] http://www.malware.lu/assets/files/articles/RAP002_APT1_Technical_backstage.1.0.pdf

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-s4gx
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0072

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Some malware sensor software is specifically designed to deliver captured malware samples to an analysis cloud. As captured malware samples may include encrypted zero day exploits inside their staging mechanisms, such sensors would be unable to determine whether they were delivering intrusion software, which leaves their classification uncertain. Please provide detail on the control level of software that delivers captured encrypted software without determining whether zero-day exploits are hidden inside the encryption.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-3dz7
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0073

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

Zero-day exploits can be attacked by zero-day exploits. Zero-day exploits that attack zero-day exploits can also be attacked by zero-day exploits. This matryoshka doll property of exploits has an infinite nesting factor in theory, though in practice has only gone 3 to 4 deep. What levels of nesting fall within the definition of intrusion software?

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 17, 2015
Status: Posted
Posted: June 18, 2015
Tracking No. 1jz-8jh7-2wbq
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0074

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mike Frantzen

Address:

14425 Penrose Pl

Suite 314

Chantilly, VA, 20151

Email: mikef@kududyn.com

Phone: 7035271230

General Comment

We note that the FAQ and the proposed rules differ in many areas. Please confirm that the FAQ is not legally binding and that only the rules apply (y/n)?

really hope you people steal the livelihoods of my colleagues as you have mine so that I may more easily convince them to take up arms and finally bring tyranny to a swift, decisive end.

Attachments

US v Auernheimer 131816p

PUBLIC SUBMISSION

As of: July 10, 2015
Received: July 06, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jtu-bmjp
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0076

Comment on FR Doc # 2015-11642

Submitter Information

Name: Richard Farina

Address:

123 South Jamestown Rd
Moon Township, PA, 15108

Email: sidhayn@gmail.com

General Comment

All over this document the term "specially designed" is used in quotes. Quoted terms are required to be defined, however, I am unable to find any definition for this one. As it stands, this rule would be unreadable as "specially designed" has no meaning at all. Even in the original Wassenaar text this term appears to be undefined, and Wassenaar specifically states that quoted terms take the definition from the list of definitions and not from standard english. "specifically designed" appears to be entirely meaningless, both in this document and in Wassenaar. Please clarify the meaning of this term or drop the quotation marks.

The previous version of this comment accidentally included an incorrect email address.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 29, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8iyz-cs0n
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0077

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

Address:

Pearl, MS, 39208

General Comment

This is completely ineffective and will accomplish nothing other than further negatively impacting american businesses involved in information security already hurt economically by the fallout of the snowden revelations.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 24, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jlu-temn
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0078

Comment on FR Doc # 2015-11642

Submitter Information

Name: Andrew Sullivan

Address:

150 Dow St
Tower 2 (Dyn)
Manchester, NH, 03101

Email: iab-chair@iab.org

Organization: Internet Architecture Board

General Comment

The Internet Architecture Board would like to draw the attention of the Industry and Security Bureau to the IAB's recent Statement on the Trade in Security Technologies. The statement can be found here: <https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-statement-on-the-trade-in-security-technologies/> and it is reprinted below for your convenience.

The IAB believes that the principles embodied in this statement are consonant with those given by the U.S. State departments Secretary Kerry, such as "An Open and Secure Internet: We must have both" <<http://www.state.gov/secretary/remarks/2015/05/242553.htm>> as well as those consistently put forward by Coordinator Chris Painter of the State Department Office of the Coordinator for Cyber Issues.

We thank you for the opportunity to comment,

Andrew Sullivan
Chair, IAB

IAB Statement on the Trade in Security Technologies

12 June 2015

The Internet Architecture Board is deeply sympathetic with the desire to enhance the security of Internet protocols, infrastructure, and Internet-connected systems. We believe, however, that efforts to enhance Internet security must proceed from a thorough knowledge of the threats against the network, its protocols, and the systems attached to it. Efforts to limit the export or transfer of Internet security technologies seem likely to limit that knowledge in ways that ultimately will frustrate the general goal of a secure and stable Internet.

The identification of vulnerabilities is a fundamental part of security practice. Restrictions on systems which perform that function will make it substantially more difficult for those performing that function to design and deploy secure systems.

Traffic analysis systems, though they may be used in other ways, are a similarly crucial part of the methods used to identify attacks and to analyze the success of remediations put in place. The Internet is a deeply interconnected set of networks that spans international borders, and attacks may occur in one part of the Internet that have extensive ramifications for the operation of the whole. Limiting traffic analysis technologies to specific territories seems likely to hinder efforts to detect and thwart both active threats and other network issues.

We note that in 1996 the IAB and Internet Engineering Steering Group (IESG) jointly published RFC 1984, with the following comments on a similar matter, the export of encryption technology:

Export controls on encryption place companies in that country at a competitive disadvantage. Their competitors from countries without export restrictions can sell systems whose only design constraint is being secure, and easy to use.

Usage controls on encryption will also place companies in that country at a competitive disadvantage because these companies cannot securely and easily engage in electronic commerce.

Export controls and usage controls are slowing the deployment of security at the same time as the Internet is exponentially increasing in size and attackers are increasing in sophistication. This puts

users in a dangerous position as they are forced to rely on insecure electronic communication.

We believe the same points to be fundamentally true for the export of traffic analysis, penetration testing, and similar security technologies.

While it may appear possible to narrowly circumscribe restrictions so that they target technologies that serve no possible purpose but attack, any modular system, including those intended solely for research, will like have some elements that, divorced from the system, would serve no other purpose. Efforts to target such systems will thus likely sweep up many other security technologies. We therefore recommend that export restrictions on security technologies be generally avoided.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 20, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jj0-v8ip
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0079

Comment on FR Doc # 2015-11642

Submitter Information

Name: Richard McCutcheon

Address:

1906 Cannon Ridge Dr
Odenton, MD, 21113

Email: Mac@macuisdein.com

Phone: 4103571749

General Comment

The definition of intrusion software (in 772.1) is so broad that it would limit cyber security research and reduce the security of the United States and its allies. The malicious use of software should be the focus not the capability.

"Exporting or importing intrusion software for the purposes of criminal activity" should be prohibited not just the import, export, or development of intrusion software.

As an instructor at the Defense Cyber Investigations Training Academy (<http://www.dc3.mil/cyber-training/about-dcita>), we train the investigators, analysts, and operators who defend the DoD and other federal agency's systems. To train them, we must use "software" "specifically designed" or modified to defeat 'protective countermeasures' that extract "data or information from a computer or network-capable device" and modify "the standard execution path of a program or process in order to allow the execution of externally provided instructions."

As defined, we require intrusion software to teach our students to find evidence of that intrusion

software being used against US Government systems. While the Academy may get exceptions under this proposed rule, our partners in Academia and the private sector may not. Permits are expensive for small groups and individuals. Yet these individuals, groups, and other partners (some domestic and some foreign) are required for the security of our nations systems.

More broadly, we need to be encouraging STEM development in our schools, colleges, and universities. The proposed rule will greatly limit the research, interest, and usefulness of the limited research that might be conducted. As a nation we will be giving up our leadership of the cyber security community. In order to continue to make secure systems, we must be able to attempt to break into those systems. Without the proper tools (intrusion software) we will be without security in the future.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 20, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jiv-4ivv
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0080

Comment on FR Doc # 2015-11642

Submitter Information

Name: Rachel Marsden

Address:

Levallois Perret, Paris, France, 92300

Email: rachelmarsden@gmail.com

Phone: 12027381891

General Comment

I'm sure that I'm in the minority here, but I fully support this new Wassenaar application . Much like Wassenaar hasn't stopped all illicit trafficking of traditional arms, it is not feasible to presume that it will stop all illicit transfers of cyber arms either. However, as with its current applications, non-compliance can serve to expose those with malicious intent. But this will ONLY be the case if registration is simple, free, and easy to navigate for the AVERAGE RESEARCHER. The moment the process becomes too complex and requires hiring of a lawyer is the moment that the average person is going to simply ignore the legislation and take their chances on getting caught. So the key is to make it extremely easy (and free) to understand the provisions and to register exploits without the assistance of legal counsel -- in which case everyone who doesn't comply is fair game. I am a Canadian citizen based in Paris, France, and an international business and political risk intelligence consultant who advises multinational clients on regulatory compliance in both transparent and opaque jurisdictions, including the navigation of Wassenaar Agreement provisions.

Attachments

Rachel Marsden Resume (6)

The attachment is restricted to show metadata only. The reason is: Non related material

PUBLIC SUBMISSION

As of: July 10, 2015 Received: June 19, 2015 Status: Posted Posted: July 10, 2015 Tracking No. 1jz-8jip-lhyk Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0081

Comment on FR Doc # 2015-11642

Submitter Information

Name: Andrew Auernheimer

Address:

none, I'm homeless now, thanks for that

Email: gluttony@gmail.com

Phone: (646) 397-1582

General Comment

I'm a somewhat distinguished information security researcher. While you have entertained the comment of those more distinguished by their achievements in the field, I believe I can offer a unique perspective out of my life experience. I think these set of changes are wonderful, and I would encourage you to make them. The reasons why may be illuminating to you.

In June of 2010, I disclosed a flaw on a web server that put AT&T iPad customers at risk. I went public with that flaw because I believe that when someone puts you at risk, you deserve to know about it so you can mitigate the risk that you have been exposed to. In January of 2011, I was kidnapped from my birthplace of Fayetteville, AR at gunpoint and taken to the third world hellhole of Newark, NJ under false pretenses. I was never allowed to return home. I was beaten, starved, and subject to solitary confinement. I no longer have a home to go back to. It has been bulldozed to clear a way for its new occupiers. An agent of the US attorney's office admitted he did not understand in a federal appeals court what I did and I was eventually set free in a precedent-setting decision, but not before you people stole three and a half years of my life under false pretenses.

I have now dedicated my life to convincing everyone I know that the only way to solve the

problem of you people is through a pogrom. These are harder to start than you may think, so I really hope you people steal the livelihoods of my colleagues as you have mine so that I may more easily convince them to take up arms and finally bring tyranny to a swift, decisive end.

Attachments

US v Auernheimer 131816p

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 13-1816

UNITED STATES OF AMERICA
v.

ANDREW AUERNHEIMER,
a/k/a Weev
a/k/a Weelos
a/k/a Escher

ANDREW AUERNHEIMER,
Appellant

On Appeal from the United States District Court
for the District of New Jersey
(No. 2:11-cr-00470-001)
District Judge: Hon. Susan D. Wigenton

Argued: March 19, 2014

Before: CHAGARES, GREENAWAY, JR., and
VANASKIE, Circuit Judges.

(Filed: April 11, 2014)

OPINION

Tor B. Ekeland, Esq.
Mark H. Jaffe, Esq.
Tor Ekeland, P.C.
155 Water Street.
Sixth Floor, Suite Two
Brooklyn, NY 11201

Orin S. Kerr, Esq. [ARGUED]
George Washington University
2000 H Street, N.W.
Washington, DC 20052

Marcia C. Hofmann, Esq.
25 Taylor Street
San Francisco, CA 94102

Hanni M. Fakhoury, Esq.
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Attorneys for Appellant

Paul J. Fishman, Esq.
Glenn J. Moramarco, Esq. [ARGUED]
Office of United States Attorney
Camden Federal Building & Courthouse
401 Market Street
Camden, NJ 08101

Mark E. Coyne, Esq.
Office of United States Attorney
970 Broad Street
Newark, NJ 07102
Attorneys for Appellee

Christopher C. Walsh, Esq.
Harvard Law School
Cyberlaw Clinic
23 Everett Street
Second Floor
Cambridge, MA 02138

Alexander C. Muentz, Esq.
Temple University
Department of Criminal Justice
1115 Pollett Walk
Philadelphia, PA 19122

Jennifer S. Granick, Esq.
Stanford Law School
Center for Internet & Society
559 Nathan Abbott Way
Stanford, CA 94305

Steven P. Ragland, Esq.
Keker & Van Nest
633 Battery Street
San Francisco, CA 94111
Attorneys for Amicus Appellants

CHAGARES, Circuit Judge.

This case calls upon us to determine whether venue for Andrew Auernheimer’s prosecution for conspiracy to violate the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030, and identity fraud under 18 U.S.C. § 1028(a)(7) was proper in the District of New Jersey. Venue in criminal cases is more than a technicality; it involves “matters that touch closely the fair administration of criminal justice and public confidence in it.” United States v. Johnson, 323 U.S. 273, 276 (1944). This is especially true of computer crimes in the era of mass interconnectivity. Because we conclude that venue did not lie in New Jersey, we will reverse the District Court’s venue determination and vacate Auernheimer’s conviction.

I.

A.

The relevant facts are fairly simple and not in dispute. Apple, Inc. introduced the first iPad, a tablet computer, in 2010. Customers who purchased the version that had the capability to send and receive data over cellular networks (commonly referred to as “3G”) had to purchase a data contract from AT&T, Inc. (“AT&T”), which at the time was the exclusive provider of data services for this version of the iPad. Customers registered their accounts with AT&T over the Internet on a website that AT&T controlled. In the registration process, customers were assigned a user identifier

(“user ID”) and created a password — login credentials that they would need in order to access their accounts through AT&T’s website in the future. The user ID assigned to each customer was that customer’s email address.

AT&T decided to make it easier for customers to log into their accounts by prepopulating the user ID field on the login screen with their email addresses. To do this, AT&T programmed its servers to search for an iPad user’s Integrated Circuit Card Identifier (“ICC-ID”) when a user directed her browser to AT&T’s general login webpage (AT&T’s “URL”¹). An ICC-ID is the unique nineteen- or twenty-digit number that identifies an iPad’s Subscriber Identity Module, commonly known as a SIM Card. The SIM Card is the computer chip that allows iPads to connect to cellular data networks.

If AT&T’s servers recognized the ICC-ID as associated with a customer who had registered her account with AT&T, then AT&T’s servers would automatically redirect the customer’s browser away from the general login URL to a different, specific URL. That new specific URL was unique for every customer and contained the customer’s ICC-ID in the URL itself. Redirecting the customer’s browser to the new specific URL told AT&T’s servers which email address to populate in the user ID field on the login page. This shortcut reduced the amount of time it took a customer to log into her account because, with her user ID already populated, she had to enter only her password.²

¹ URL is shorthand for uniform resource locator, which is defined as “a specific address . . . used by a browser in locating the relevant document [on the Internet].” URL, Oxford Eng. Dictionary, <http://www.oed.com/view/Entry/258858?redirectedFrom=URL#eid> (last visited Mar. 27, 2014). It is more commonly known as a “web address.” Appendix (“App.”) 255.

² To make this more concrete, when an iPad user wanted to log into her account, she would direct her browser to “https://dcp2.att.com/OEPNDClient?”. If AT&T’s server recognized the ICC-ID of the iPad that made the request as an iPad that was already registered with AT&T, its servers would automatically redirect the user to

Daniel Spitler, Auernheimer's co-conspirator, discovered this feature of AT&T's login process. Although he did not own an iPad, he purchased an iPad SIM Card, hoping to install it on another computing device and then take advantage of the unlimited cellular data plan that AT&T offered for \$30 per month. At first, he did not know how to register his SIM Card, so he downloaded the iPad operating system onto his computer, decrypted it, and browsed through the operating system's code to try to find a way to register it. In the course of doing so, he came across AT&T's registration URL. He noticed that one of the variables in the registration URL was a field requiring an ICC-ID.

Spitler then directed his computer's web browser to the registration URL and inserted his iPad's ICC-ID in the requisite place. AT&T's servers were programmed only to permit browsers that self-identified as iPad browsers to access the registration URL. This required him to change his browser's user agent. A user agent tells a website what kind of browser and operating system a user is running, so servers that someone is attempting to access can format their responses appropriately. App. 256.

After changing his browser's user agent to appear as an iPad, Spitler was able to access the AT&T login page. He noticed that his email address was already populated in the login field and surmised that AT&T's servers had tied his email address to his ICC-ID. He tested this theory by changing the ICC-ID in the URL by one digit and discovered that doing so returned a different email address. He changed the ICC-ID in the URL manually a few more times, and each time the server returned other email addresses in the login field.

Spitler concluded that this was potentially a noteworthy security flaw. He began to write a program that he called an "account slurper" that would automate this process. The account slurper would repeatedly access the

"https://dcp2.att.com/OEPNDClient/openPage?ICCID=XXX
XXXXXXXXXXXXXXXXXXXX&IMEI=0", where the string of
"X"s is the nineteen- or twenty-digit ICC-ID.

AT&T website, each time changing the ICC-ID in the URL by one digit. If an email address appeared in the login box, the program would save that email address to a file under Spitler's control.

Spitler shared this discovery with Auernheimer, whom he knew through Internet-based chat rooms but had never met in person. Auernheimer helped him to refine his account slurper program, and the program ultimately collected 114,000 email addresses between June 5 and June 8, 2010. Its method — guessing at random — is called a “brute force” attack, a term of art in the computer industry referring to an inefficient method of simply checking all possible numbers.

While Spitler's program was still collecting email addresses, Auernheimer emailed various members of the media in order to publicize the pair's exploits. Some of those media members emailed AT&T, which immediately fixed the breach. One of the media members contacted by Auernheimer was Ryan Tate, a reporter at Gawker, a news website. Tate expressed interest in publishing Auernheimer's story. To lend credibility to it, Auernheimer shared the list of email addresses with him. Tate published a story on June 9, 2010 describing AT&T's security flaw, entitled “Apple's Worst Security Breach: 114,000 iPad Owners Exposed.” The article mentioned some of the names of those whose email addresses were obtained, but published only redacted images of a few email addresses and ICC-IDs.

Evidence at trial showed that at all times relevant to this case, Spitler was in San Francisco, California and Auernheimer was in Fayetteville, Arkansas. The servers that they accessed were physically located in Dallas, Texas and Atlanta, Georgia. Although no evidence was presented regarding the location of the Gawker reporter, it is undisputed that he was not in New Jersey.

B.

Despite the absence of any apparent connection to New Jersey, a grand jury sitting in Newark returned a two-count superseding indictment charging Auernheimer with conspiracy to violate the CFAA, 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B)(ii), in violation of 18 U.S.C. § 371 (count one),

and fraud in connection with personal information in violation of 18 U.S.C. § 1028(a)(7) (count two, commonly referred to as “identity fraud”). To enhance the potential punishment from a misdemeanor to a felony, the Government alleged that Auernheimer’s CFAA violation occurred in furtherance of a violation of New Jersey’s computer crime statute, N.J. Stat. Ann. § 2C:20-31(a). See 18 U.S.C. § 1030(c)(2)(B)(ii).

Auernheimer moved to dismiss the superseding indictment shortly after it was returned by the grand jury. In addition to asserting several challenges concerning the CFAA violation, he argued that venue was not proper in the District of New Jersey. The District Court acknowledged that neither he nor Spitler was ever in New Jersey while allegedly committing the crime, and that the servers accessed were not in New Jersey, but denied his motion nonetheless. It held that venue was proper for the CFAA conspiracy charge because Auernheimer’s disclosure of the email addresses of about 4,500 New Jersey residents affected them in New Jersey and violated New Jersey law. It further held that because venue was proper for the CFAA count, it was also proper for the identity fraud count because proving the CFAA violation was a necessary predicate to proving the identity fraud violation.

Auernheimer’s trial lasted five days and resulted in a guilty verdict on both counts. Initially, both parties requested a jury instruction on venue. App. 575. Venue is a question for the jury and the court “must specifically instruct the jury on venue” if “(1) the defendant objects to venue prior to or at the close of the prosecution’s case-in-chief, (2) there is a genuine issue of material fact with regard to proper venue, and (3) the defendant timely requests a jury instruction.” United States v. Perez, 280 F.3d 318, 334 (3d Cir. 2002). Although Auernheimer objected to venue and requested an instruction, the District Court held that there was no genuine issue of material fact. It concluded that the Government had established that venue was proper in New Jersey as a matter of law and declined to instruct the jury on venue. App. 591.

After denying Auernheimer’s post-trial motions, the District Court sentenced him to forty-one months of imprisonment. Auernheimer timely appealed.

II.

The District Court had jurisdiction pursuant to 18 U.S.C. § 3231. We have jurisdiction pursuant to 28 U.S.C. § 1291. Our review of the District Court's legal decision regarding venue is plenary. United States v. Pendleton, 658 F.3d 299, 302 (3d Cir. 2011).

III.

Although this appeal raises a number of complex and novel issues that are of great public importance in our increasingly interconnected age, we find it necessary to reach only one that has been fundamental since our country's founding: venue. The proper place of colonial trials was so important to the founding generation that it was listed as a grievance in the Declaration of Independence. See The Declaration of Independence para. 21 (U.S. 1776) (objecting to "transporting us beyond seas to be tried for pretended offences"). It was of such concern that the Constitution of the United States "twice safeguards the defendant's venue right." United States v. Cabrales, 524 U.S. 1, 6 (1998). Article III requires that "the Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Sixth Amendment further provides that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." Id. amend VI. This guarantee is codified in the Federal Rules of Criminal Procedure, which require that "the [G]overnment must prosecute an offense in a district where the offense was committed." Fed. R. Crim. P. 18.

Congress may prescribe specific venue requirements for particular crimes. Pendleton, 658 F.3d at 303. Where it has not, as is the case here, we must determine the crime's locus delicti. Id.; see also Black's Law Dictionary 1025 (9th ed. 2009) (defining locus delicti as the "place where an offense was committed"). "[T]he locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it." United States v. Anderson, 328 U.S. 699, 703 (1946); accord United States v.

Rodriguez-Moreno, 526 U.S. 275, 279 (1999); Cabrales, 524 U.S. at 6-7. To perform this inquiry, we “must [1] initially identify the conduct constituting the offense . . . and then [2] discern the location of the commission of the criminal acts.” Rodriguez-Moreno, 526 U.S. at 279. Venue should be narrowly construed. Johnson, 323 U.S. at 276.

Continuing offenses, such as conspiracy, that are “begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed.” 18 U.S.C. § 3237(a). In the context of a conspiracy charge, “venue can be established wherever a co-conspirator has committed an act in furtherance of the conspiracy.” Perez, 280 F.3d at 329; accord Hyde v. United States, 225 U.S. 347, 356-67 (1912). The Government must prove venue by a preponderance of the evidence. United States v. Root, 585 F.3d 145, 155 (3d Cir. 2009).

In performing our venue inquiry, we must be careful to separate “essential conduct elements” from “circumstance element[s].” Rodriguez-Moreno, 526 U.S. at 280 & n.4. For example, in Cabrales the Supreme Court considered whether venue for money laundering activities was proper in Missouri. 524 U.S. at 4. The laundered proceeds were generated by illegal narcotics sales in Missouri, but all acts constituting the money laundering offense took place in Florida. Id. The Court held that venue was improper in Missouri. Id. at 10. The Supreme Court, later reflecting on Cabrales, observed that the “existence of criminally generated proceeds” was only a “circumstance element” of money laundering. Rodriguez-Moreno, 526 U.S. at 280 n.4. Although it was an element of the crime that the Government had to prove to the jury, it was a “circumstance element” because it was simply a fact that existed at the time that the defendant performed her laundering acts. Only “essential conduct elements” can provide the basis for venue; “circumstance elements” cannot. United States v. Bowens, 224 F.3d 302, 310 (4th Cir. 2000).

A.

Count one charged Auernheimer with conspiracy to violate CFAA § 1030(a)(2)(C) and (c)(2)(B)(ii). In the

indictment and at trial, the Government identified the nature of the conduct constituting the offense as the agreement to commit a violation of the CFAA in furtherance of a violation of New Jersey's computer crime statute, N.J. Stat. Ann. § 2C:20-31(a). Venue would be proper in any district where the CFAA violation occurred, or wherever any of the acts in furtherance of the conspiracy took place. See Perez, 280 F.3d at 329; see also Rodriguez-Moreno, 526 U.S. at 281-82 (citing Hyde, 225 U.S. at 356-67).

The charged portion of the CFAA provides that “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.” 18 U.S.C. § 1030(a)(2)(C). To be found guilty, the Government must prove that the defendant (1) intentionally (2) accessed without authorization (or exceeded authorized access to) a (3) protected computer and (4) thereby obtained information. See United States v. Willis, 476 F.3d 1121, 1125 (10th Cir. 2007) (delineating the elements in a similar manner). The statute's plain language reveals two essential conduct elements: accessing without authorization and obtaining information.³

New Jersey was not the site of either essential conduct element. The evidence at trial demonstrated that the accessed AT&T servers were located in Dallas, Texas, and Atlanta, Georgia. App. 443-44. In addition, during the time that the conspiracy began, continued, and ended, Spitler was obtaining information in San Francisco, California (App. 233), and Auernheimer was assisting him from Fayetteville, Arkansas (App. 366). No protected computer was accessed and no data was obtained in New Jersey.

³ The Department of Justice's own manual on prosecuting computer crimes provides in its section devoted to venue that “it would seem logical that a crime under section 1030(a)(2)(C) is committed where the offender initiates access and where the information is obtained.” Computer Crime & Intellectual Prop. Section, Dep't of Justice, Prosecuting Computer Crimes 118, available at <http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf> (last visited Mar. 26, 2014) (“DOJ Manual”).

This is not the end of our analysis, however, because the Government did not just charge Auernheimer with conspiracy to commit an ordinary violation of the CFAA, but also with conspiring to violate the CFAA in furtherance of a state crime. The Government can increase the statutory maximum punishment for a subsection (a)(2) violation from one year to five years if it proves one of the enhancements contained in § 1030(c)(2)(B). The enhancement relevant here provides for such increased punishment if “the offense was committed in furtherance of any criminal or tortious act in violation of the . . . laws of . . . any State.” *Id.* § 1030(c)(2)(B)(ii). “[A]ny ‘facts that increase the prescribed range of penalties to which the criminal defendant is exposed’ are elements of the crime” that must be proven to the jury beyond a reasonable doubt.⁴ *Alleyne v. United States*, 133 S. Ct. 2151, 2160 (2013) (quoting *Apprendi v. New Jersey*, 530 U.S. 466, 490 (2000)). This is true even if they are explicitly termed “sentence enhancement[s]” in the statute. *Apprendi*, 530 U.S. at 494 n.19 (quotation marks omitted).

The New Jersey statute allows for criminal liability “if the person purposely or knowingly and without authorization, or in excess of authorization, accesses any . . . computer [or] computer system and knowingly or recklessly discloses, or causes to be disclosed any data . . . or personal identifying information.” N.J. Stat. Ann. § 2C:20-31(a). Its essential conduct elements are accessing without authorization (or in excess of authorization) and disclosing data or personal identifying information.

Here, none of the essential conduct elements of a violation of the New Jersey statute occurred in New Jersey. As discussed, neither Auernheimer nor Spitler accessed a

⁴ Just because the enhancement is an “element” that the Government needed to prove beyond a reasonable doubt does not mean that it was an “essential conduct element” of a § 1030(a)(2)(C) violation within the meaning of *Rodriguez-Moreno* that could establish venue. For the purposes of this opinion, however, we will assume (without deciding) that the enhancement could contain “essential conduct elements.”

computer in New Jersey.⁵ The disclosure did not occur there either. The sole disclosure of the data obtained was to the Gawker reporter. There was no allegation or evidence that the Gawker reporter was in New Jersey. Further, there was no evidence that any email addresses of any New Jersey residents were ever disclosed publicly in the Gawker article. The alleged violation of the New Jersey statute thus cannot confer venue for count one.

Just as none of the conduct constituting the CFAA violation or its enhancement occurred in New Jersey, none of the overt acts that the Government alleged in the superseding indictment occurred in New Jersey either. The indictment listed four overt acts: writing the account slurper program, deploying the account slurper program against AT&T's servers, emailing victims to inform them of the breach, and disclosing the emails addresses obtained to Gawker. The co-conspirators collaborated on the account slurper program from California and Arkansas and deployed it against servers located in Texas and Georgia. The Government offered no evidence whatsoever that any of the victims that Auernheimer emailed were located in New Jersey, or that the Gawker reporter to whom the list of email addresses was disclosed was in the Garden State.

Because neither Auernheimer nor his co-conspirator Spitler performed any "essential conduct element" of the underlying CFAA violation or any overt act in furtherance of the conspiracy in New Jersey, venue was improper on count one.

⁵ We also note that in order to be guilty of accessing "without authorization, or in excess of authorization" under New Jersey law, the Government needed to prove that Auernheimer or Spitler circumvented a code- or password-based barrier to access. See State v. Riley, 988 A.2d 1252, 1267 (N.J. Super. Ct. Law Div. 2009). Although we need not resolve whether Auernheimer's conduct involved such a breach, no evidence was advanced at trial that the account slurper ever breached any password gate or other code-based barrier. The account slurper simply accessed the publicly facing portion of the login screen and scraped information that AT&T unintentionally published.

B.

We now turn to count two of the indictment because venue must be analyzed independently for each count. See Root, 585 F.3d at 155. Count two charged Auernheimer with violating 18 U.S.C. § 1028(a)(7), which punishes anyone who “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any [federal crime, or state or local felony].” The statute’s plain language indicates that the statute punishes someone who (1) knowingly (2) transfers, possesses, or uses without lawful authority (3) a means of identification of another person (4) with the intent to commit, or in connection with, any violation of federal law or any state felony. See United States v. Abdelshafi, 592 F.3d 602, 607 (4th Cir. 2010) (delineating the elements of a violation of aggravated identity fraud in 18 U.S.C. § 1028A(a)(1), which are virtually identical, in a similar fashion); United States v. Stephens, 571 F.3d 401, 404-05 (5th Cir. 2009) (same).

The two essential conduct elements under § 1028(a)(7) are transfer, possession, or use, and doing so in connection with a federal crime or state felony. Cf. Rodriguez-Moreno, 526 U.S. at 280 (noting that “during and in relation to any crime of violence” was an essential conduct element of a firearms statute). Starting with the latter essential conduct element, the Government charged Auernheimer with committing identity fraud “in connection with” the ordinary violation of CFAA § 1030(a)(2)(C). As should be clear by now, no conduct related to the ordinary CFAA violation occurred in New Jersey.

There was also no evidence that Auernheimer’s transfer, possession, or use occurred in New Jersey. The Government advances two theories of how he could have satisfied this essential conduct element. First, it contends that he violated § 1028(a)(7) by knowingly using the ICC-IDs of other people’s iPads to access AT&T’s servers. See Gov’t Br. 64-66. Venue fails under this theory because there was no allegation or evidence that he used the ICC-IDs in New Jersey. The alleged conspirators used the ICC-IDs in their

account slurper program, which was programmed from California and Arkansas, and did not access any computer or obtain any information in New Jersey.

The Government also argues that Auernheimer violated the statute by transferring the list of email addresses that he obtained to Gawker with the intent to violate the New Jersey computer crime statute. See Gov't Br. 67-69. But there was no allegation in the indictment or evidence at trial that the Gawker reporter to whom he transferred the email addresses was in New Jersey — and no essential conduct element of the alleged violation of New Jersey law occurred in New Jersey either.⁶

Because Auernheimer did not commit any essential conduct of the identity fraud charge in New Jersey, venue was also improper on count two.

IV.

The Government does not dispute the locations of Auernheimer, Spitler, and AT&T's servers during the period of time that Auernheimer was committing the alleged crimes. Instead, it advances a series of other reasons why there was no defect in venue that warrants vacating his conviction. None of them are availing.

A.

The Government argues that we need not rely on the essential conduct elements test mandated by Cabrales and Rodriguez-Moreno because we have “adopted,” Gov't Br. 71,

⁶ Further, count two of the indictment charged Auernheimer with transferring, possessing, and using the means of identification of others in connection with only an ordinary violation of CFAA § 1030(a)(2)(C). It did not mention the violation of New Jersey law or the § 1030(c)(2)(B)(ii) enhancement at all. This second theory thus “broaden[s] the possible bases for conviction from that which appeared in the indictment.” United States v. McKee, 506 F.3d 225, 229 (3d Cir. 2007) (quotation marks omitted). It cannot be a permissible basis upon which to find venue for count two.

a “substantial contacts test.” Under this approach, frequently employed by the Court of Appeals for the Second Circuit, a number of factors help to determine whether venue was proper, including “the site of the defendant’s acts, the elements and nature of the crime, the locus of the effect of the criminal conduct, and the suitability of each district for accurate factfinding.” United States v. Reed, 773 F.2d 477, 481 (2d Cir. 1985). The Government contends that venue is proper in New Jersey because about four percent (approximately 4,500 of 114,000) of the email addresses obtained from AT&T’s website belonged to New Jersey residents, thereby satisfying the “locus of the effect[s]” consideration. See id.

It is far from clear that this Court has ever “adopted” this test. We have mentioned it only once. See United States v. Goldberg, 830 F.2d 459, 466 (3d Cir. 1987). The test was cited in a long block quote to Reed, and then analyzed in a single sentence. Id. The Goldberg panel did not need to rely on the locus of the effects of the defendant’s conduct in that case because all of his acts took place in the district in which he was tried. Id. No panel of this Court has ever cited Goldberg, or any other case, for this test since — either before, or especially after, the Supreme Court clarified the venue inquiry in Cabrales and Rodriguez-Moreno.

Even if it could be said that we perhaps tacitly endorsed this test once almost thirty years ago, the test operates to limit venue, not to expand it. Cases from the Court of Appeals for the Second Circuit make this clear. The test “does not represent a formal constitutional test,” but rather is merely “helpful in determining whether a chosen venue is unfair or prejudicial to a defendant.” United States v. Saavedra, 223 F.3d 85, 93 (2d Cir. 2000). To satisfy this test, there must be “more than ‘some activity in the situs district’; instead, there must be ‘substantial contacts.’” United States v. Davis, 689 F.3d 179, 186 (2d Cir. 2012) (quoting Reed, 773 F.2d at 481). There “must be some sense of venue having been freely chosen by the defendant.” Id. (alteration and quotation marks omitted). If a defendant argues that the chosen venue is constitutionally infirm but that it did not result in any hardship to him, the court only determines the locus delicti and does not then analyze

whether there were “substantial contacts.” See United States v. Magassouba, 619 F.3d 202, 205 n.2 (2d Cir. 2010). This test thus serves to limit venue in instances where the locus delicti constitutionally allows for a given venue, but trying the case there is somehow prejudicial or unfair to the defendant.

Even assuming that the substantial contacts test is viable within our Circuit, it cannot serve as a sufficient basis for conferring venue. The Government argues only that it has minimally satisfied one of the four prongs of the test — the “locus of the effect of the criminal conduct.” There was no evidence at trial that Auernheimer’s actions evinced any contact with New Jersey, much less contact that was “substantial.” The Government has not cited, and we have not found, any case where the locus of the effects, standing by itself, was sufficient to confer constitutionally sound venue.

Undoubtedly there are some instances where the location in which a crime’s effects are felt is relevant to determining whether venue is proper. See Rodriguez-Moreno, 526 U.S. at 279 n.2 (reserving the issue of whether venue may also be permissibly based on the location where a crime’s effects are felt). But those cases are reserved for situations in which “an essential conduct element is itself defined in terms of its effects.” Bowens, 224 F.3d at 311. For example, in a prosecution for Hobbs Act robbery, venue may be proper in any district where commerce is affected because the terms of the act themselves forbid affecting commerce. See 18 U.S.C. § 1951(a); accord United States v. Smith, 198 F.3d 377, 383 (2d Cir. 1999). This is consistent with Congress’s prerogative to “provide that the locality of a crime shall extend over the whole area through which force propelled by an offender operates.” Johnson, 323 U.S. at 275.

Sections of the CFAA other than § 1030(a)(2)(C) do speak in terms of their effects. For example, § 1030(a)(5)(B) criminalizes intentionally accessing a computer without authorization and recklessly causing damage. Because that

crime is defined in terms of its effects — the damage caused — venue could be proper wherever that occurred.⁷

Congress, however, did not define a violation of § 1030(a)(2)(C) in terms of its effects. The statute simply criminalizes accessing a computer without authorization and obtaining information. It punishes only the actions that the defendant takes to access and obtain. It does not speak in terms of the effects on those whose information is obtained. The crime is complete even if the offender never looks at the information and immediately destroys it, or the victim has no idea that information was ever taken.

B.

The Government also argues that venue was proper in New Jersey because Auernheimer failed to obtain authorization from approximately 4,500 New Jersey residents to “use[] their ICC-ID numbers to access the AT&T servers.” Gov’t Br. 80. The Government argues that when a statute makes it a crime to fail to do some required act, venue can lie in the district in which the act should have been done. The Government concludes that venue is proper because Auernheimer and Spitler failed to obtain authorization from about 4,500 people in New Jersey prior to accessing AT&T’s servers.

This rule only applies, however, when a preexisting legal duty requires the act that the defendant failed to do. See 1 Wayne R. LaFare, Substantive Criminal Law § 6.2(a) (2d ed. 2003) (noting that crimes of omission are generally limited by specific duties such as relationship, statute, contract, assumption of care, creation of peril, controlling the conduct of others, and landowner); accord United States v. Sabhnani, 599 F.3d 215, 237 (2d Cir. 2010). Failure to

⁷ The Department of Justice manual again tailors its guidance to this assessment, noting that a prosecution under § 1030(a)(5) “may be brought where the effects are felt because those charges are defined in terms of ‘loss,’ even if the bulk of network crimes may not be prosecuted in a district simply because the effects of the crime are felt there.” DOJ Manual at 120.

perform a required act could confer venue where a defendant should have performed that act when a statute penalizes inaction, such as failure to report to a military draft board (see, e.g., Johnston v. United States, 351 U.S. 215, 219-20 (1956)), failure to report to prison after being sentenced (see, e.g., United States v. Overaker, 766 F.2d 1326, 1327 (9th Cir. 1985)), or failure to file income tax returns (see, e.g., United States v. Garman, 748 F.2d 218, 219 (4th Cir. 1984)). Here, Auernheimer was under no such preexisting duty — legal or otherwise. Like most statutes, the charged portion of the CFAA punishes affirmative acts, not inaction. His failure to obtain authorization cannot confer venue in every district in which a potential victim lived.

C.

Finally, the Government argues that even if venue were improper, we should apply harmless error analysis and disregard the error because it did “not affect substantial rights.” Fed. R. Crim. P. 52(a). Although the Government makes this argument only in passing — it occupies less than one page of its 118-page brief — we feel obliged to address it. The Government contends that its choice of forum actually benefitted Auernheimer, because locating his trial in Newark, New Jersey “enhance[d] his ability to attract and retain experienced and capable counsel on a pro bono basis.” Gov’t Br. 98; see also id. at 97 (noting that Newark was a “relatively easy commute” for Auernheimer’s attorney from his office in Brooklyn, New York).

At the outset, we are skeptical that venue errors are susceptible to harmless error analysis. The Supreme Court has divided constitutional errors into two classes: “trial” and “structural.” Arizona v. Fulminante, 499 U.S. 279, 307-10 (1991). Trial errors occur “during the presentation of the case to the jury” and can be “quantitatively assessed in the context of other evidence presented” in order to determine whether they are “harmless beyond a reasonable doubt.” Id. at 307-08. These include “most constitutional errors.” Id. at 306. Structural errors “defy” harmless error analysis because they “affect[] the framework within which the trial proceeds,” id. at 309-10, “or indeed [] whether it proceeds at all,” United States v. Gonzalez-Lopez, 548 U.S. 140, 150 (2006). These

include a “limited class of fundamental constitutional errors,” Neder v. United States, 527 U.S. 1, 7 (1999), such as the denial of the rights to counsel, self-representation, or a public trial. See Gonzales-Lopez, 548 U.S. at 149 (listing examples and authority).

An error regarding venue exhibits many of the characteristics of structural error. If the District Court had found venue lacking upon Auernheimer’s motion to dismiss, there would have been no trial in New Jersey at all. Even if venue had been raised only at trial, “if venue is improper no constitutionally valid verdict could be reached regardless of the [potentially] overwhelming evidence against the defendant.” United States v. Miller, 111 F.3d 747, 757 (10th Cir. 1997) (Barrett, J., dissenting). The error thus “def[ies] analysis by harmless-error standards by affecting the entire adjudicatory framework.” Puckett v. United States, 556 U.S. 129, 141 (2009) (quotation marks omitted). Holding that defective venue could ever be harmless would arguably reduce this constitutional protection to a nullity because, under the Government’s formulation, the error would be harmless as long as the evidence against the accused of the substantive crime was overwhelming. It is doubtful that this is the way the venue protections in the Constitution were meant to operate. See also 4 Wayne R. LaFave et al., Criminal Procedure § 16.1(g) (4th ed. 2007) (“Failure of venue will not be treated as harmless error.”).

The Supreme Court has never held that improper venue is subject to harmless error review. The Government has pointed to only one case where a court subjected defective venue to harmless error review. See United States v. Hart-Williams, 967 F. Supp. 73, 78-81 (E.D.N.Y. 1997). In Hart-Williams, the district court found the venue error harmless after the defendant was convicted at a courthouse in Brooklyn, New York, that was less than a mile from the courthouse where venue would have been proper in Manhattan, New York. See id. at 80. No court has cited Hart-Williams for this proposition, and the Court of Appeals for the Second Circuit has cast doubt on whether the district court’s application of harmless error review remains good law. See United States v. Brennan, 183 F.3d 139, 149 (2d Cir. 1999) (holding that trial in Brooklyn, New York, where

venue was improper, was not harmless when the defendant timely objected to venue, even though venue would have been proper in Manhattan, New York); see also Saavedra, 223 F.3d at 100 n.5 (Cabranes, J., dissenting) (explicitly noting that Brennan forecloses applying harmless error analysis to defective venue).

Nonetheless, even assuming that defective venue could be amenable to harmless error review, the venue error here clearly affected Auernheimer's substantial rights. In order for an error to be harmless, "the Government must 'prove beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained.'" Gov't of V.I. v. Davis, 561 F.3d 159, 165 (3d Cir. 2009) (quoting Chapman v. California, 386 U.S. 18, 24 (1967)). The question "is not whether, in a trial that occurred without the error, a guilty verdict would surely have been rendered, but whether the guilty verdict actually rendered in this trial was surely unattributable to the error." Sullivan v. Louisiana, 508 U.S. 275, 279 (1993). The venue error in this case is not harmless because there was no evidence that any of the essential conduct elements occurred in New Jersey. If Auernheimer's jury had been properly instructed on venue, it could not have returned a guilty verdict; the verdict rendered in this trial would have been different. See United States v. Durades, 607 F.2d 818, 820 (9th Cir. 1979) (failing to try defendant in district where crime was allegedly committed infringed the defendant's substantial rights); see also United States v. Glenn, 828 F.2d 855, 860 (1st Cir. 1987) (same); United States v. Stratton, 649 F.2d 1066, 1076 n.15 (5th Cir. 1981) ("A defendant's interest in being tried only in a district where venue properly lay clearly constitutes a substantial right." (quotation marks omitted)).

The Supreme Court has repeatedly made clear that the constitutional limitations on venue are extraordinarily important. "[Q]uestions of venue are more than matters of mere procedure. They raise deep issues of public policy in the light of which legislation must be construed." Travis v. United States, 364 U.S. 631, 634 (1961) (quotation marks omitted). "The provision for trial in the vicinity of the crime is a safeguard against the unfairness and hardship involved when an accused is prosecuted in a remote place." United

States v. Cores, 356 U.S. 405, 407 (1958); accord United States v. Passodelis, 615 F.2d 975, 977 (3d Cir. 1980). The founders were so concerned with the location of a criminal trial that they placed the venue requirement, which is “principally a protection for the defendant,” Cabrales, 524 U.S. at 9, in the Constitution in two places. See U.S. Const. art. III, § 2, cl. 3 and amend. VI.

They did so for good reason. A defendant who has been convicted “in a distant, remote, or unfriendly forum solely at the prosecutor’s whim,” United States v. Salinas, 373 F.3d 161, 164 (1st Cir. 2004), has had his substantial rights compromised. Auernheimer was hauled over a thousand miles from Fayetteville, Arkansas to New Jersey. Certainly if he had directed his criminal activity toward New Jersey to the extent that either he or his co-conspirator committed an act in furtherance of their conspiracy there, or performed one of the essential conduct elements of the charged offenses there, he would have no grounds to complain about his uprooting. But that was not what was alleged or what happened. While we are not prepared today to hold that an error of venue never could be harmless,⁸ we do not need to because the improper venue here — far from where he performed any of his allegedly criminal acts —

⁸ We note that we are not dealing with a situation where the error complained of is that the trial judge failed to instruct the jury on venue. That claim may be reviewed for harmless error. See United States v. Casch, 448 F.3d 1115, 1117-18 (9th Cir. 2006) (noting that when proof of venue is clear, failure to instruct the jury can be considered harmless error); United States v. Martinez, 901 F.2d 374, 377 (4th Cir. 1990) (same); United States v. Moeckly, 769 F.2d 453, 461 (8th Cir. 1985) (same). In that situation, the failure to instruct would be harmless if the Government demonstrates under the Chapman standard that sufficient evidence of venue existed such that the jury would have come to that conclusion too. Cf. Neder, 527 U.S. at 7-11 (holding that an erroneous jury instruction that omitted an element of the offense is subject to harmless error analysis). The question that we address today is whether a venue defect could be harmless when there is no possibility that the jury could have found venue proper.

denied Auernheimer’s substantial right to be tried in the place where his alleged crime was committed.⁹

V.

Venue issues are animated in part by the “danger of allowing the [G]overnment to choose its forum free from any external constraints.” Salinas, 373 F.3d at 169-70 (citing Travis, 364 U.S. at 634). The ever-increasing ubiquity of the Internet only amplifies this concern. As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and computers still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no “essential conduct element” of the crimes charged. Rodriguez-Moreno, 526 U.S. at 280.

“Though our nation has changed in ways which it is difficult to imagine that the Framers of the Constitution could have foreseen, the rights of criminal defendants which they sought to protect in the venue provisions of the Constitution are neither outdated nor outmoded.” Passodelis, 615 F.2d at 977. Just as this was true when we decided Passodelis in 1980 — after the advent of railroad, express mail, the telegraph, the telephone, the automobile, air travel, and satellite communications — it remains true in today’s Internet age. For the forgoing reasons, we will reverse the District Court’s venue determination and vacate Auernheimer’s conviction.

⁹ We in no way imply that venue cannot be waived by the defendant by failing to object to it in a timely fashion. See Perez, 280 F.3d at 328. Because Auernheimer explicitly moved to dismiss the indictment for lack of venue, there is no contention that he waived his venue right here.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: June 19, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jih-9xld
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0082

Comment on FR Doc # 2015-11642

Submitter Information

Name: Howard Ehrlich

Address:

4416 East West Highway, Suite 310

Bethesda, MD, 20814

Email: howard.ehrlich@fidelissecurity.com

Phone: 3012045697

General Comment

See attached file(s)

Attachments

Signed Comments to Proposed Rule RIN 0694-AG49

June 19, 2015

Submitted via www.regulations.gov

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B, U.S. Department of Commerce
14th St and Pennsylvania Ave NW
Washington, DC 20230

By email to: publiccomments@bis.doc.gov

Re: RIN 0694-AG49

To Whom It May Concern,

This letter is in response to proposed rule RIN 0694-AG49. As a matter of context, I have included background information about our company and products.

Fidelis XPS™ is the only Comprehensive Advanced Threat Defense solution that stops advanced threats with industry-leading network traffic and payload analysis across all phases of the threat lifecycle. By focusing on real-time detection and prevention, Fidelis XPS delivers the following benefits:

- Lower enterprise risk through robust network visibility and prevention
- Lower incident response costs with fewer occurrences and faster remediation with one-click access to the “who, what, where, when, why, and how” of an attack
- Lower network security infrastructure costs through consolidation of the defense in depth stack
- Lower operational cost with automated rules and real-time threat intelligence provided through the Fidelis Insight Threat Intelligence Cloud
- Gain proactive situational awareness and prevention in real-time with actionable threat intelligence
- Achieve higher detection rate of all types of network threats, including advanced malware, exploits, spear phishing attacks, and data theft, by monitoring all phases of the threat lifecycle
- Scale to security team needs and requirements

Designed to handle the most demanding network environments, the Fidelis XPS patented Deep Session Inspection® technology powers sensors placed around the network to detect and/or prevent insider threats and advanced cyber attacks, as well as stop the final phase of attack, the theft of company data.

Delivered as a preconfigured network or virtual appliance, Fidelis XPS increases analysts' time to focus on what matters by bringing important data to the forefront and providing a single solution to discover, investigate, and contain an attack.

(Comments on next page)

Comments to Proposed Rule

Fidelis products are currently classified as 5A002.a.1 when embedded on a server and as 5D002C.1 as software only and as such are eligible for license exception ENC (unrestricted).

Fidelis relies on license exception ENC to fulfill customer sales as well as deploy product to prospective customers outside of the United States. Our resellers, all of which have undergone extensive due diligence and screening prior to execution of reseller contracts, receive product and maintain a pool of evaluation equipment to deploy on prospective customer sites. Such prospective customers undergo extensive due diligence prior to deploying evaluation equipment.

If Fidelis were to lose that ability to utilize the ENC license exception to export and re-export this would impose tremendous burden to obtain licensing for each and every evaluation conducted as well as for all product sales. Fidelis would have to hire additional labor tasked solely with managing the export licensing for evaluation product. This would be a very great financial burden that Fidelis is not in a position to absorb.

Fidelis fulfills its obligations to report self-classifications, ENC use and exports to Customs, Census, BIS, NSA and all other Governmental agencies as required. The proposed rule would cause significant difficulty and greatly alter our current and future market and sales strategy. As a relatively small company, this would cause Fidelis hardship that may very well be irreparable as we work to grow in the international market.

It is our sincere hope that the Department of Commerce Bureau of Industry and Security will amend the proposed rule so as to not create undue hardship on Fidelis Cybersecurity, Inc as well as our industry partners subject to similar regulations.

Please contact me with any questions that you may have at howard.ehrlich@fidelissecurity.com or 301-841-6494.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Howard Ehrlich', written over a white background.

Howard Ehrlich
Assistant General Counsel
Fidelis Cybersecurity, Inc.

PUBLIC SUBMISSION

As of: July 10, 2015
Received: July 06, 2015
Status: Posted
Posted: July 10, 2015
Tracking No. 1jz-8jtu-6ebm
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0083

Comment on FR Doc # 2015-11642

Submitter Information

Name: Richard Farina

Address:

123 South Jamestown Rd

Moon Township, PA, 15108

Email: sidhay@gmail.com

General Comment

All over this document the term "specially designed" is used in quotes. Quoted terms are required to be defined, however, I am unable to find any definition for this one. As it stands, this rule would be unreadable as "specially designed" has no meaning at all. Even in the original Wassenaar text this term appears to be undefined, and Wassenaar specifically states that quoted terms take the definition from the list of definitions and not from standard english.

"specifically designed" appears to be entirely meaningless, both in this document and in Wassenaar. Please clarify the meaning of this term or drop the quotation marks.

PUBLIC SUBMISSION

As of: 7/17/15 3:30 PM
Received: July 11, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8jx3-bj4o
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0085

Comment on FR Doc # 2015-11642

Submitter Information

Name: James Gannon

Address:

2 Northumberland Place

Dun Laoghaire, Dublin, Ireland,

Email: james@cyberinvasion.net

Phone: 0861753581

Organization: Cyberinvasion Ltd

General Comment

Please see attached file.

Attachments

BiSWassenaarComments

*Comments to the Department of Commerce - Bureau of Industry and Security,
Implementation of the Wassenaar Arrangement*

Cyber Invasion Ltd

09 Jul 2015

Introduction

Cyber Invasion Ltd is a security and risk management consultancy based in Dublin, Ireland. We provide security advisory services to a range of clients including Fortune 500 companies and Small and Medium enterprises.

Problem Statement

The proposed language for the implementation of the recent additions to the Wassenaar arrangement pose serious concerns to the security community about their ability to continue to be a critical part of securing global infrastructure and services.

Summary

We believe that the proposed implementation of the recent additions to the Wassenaar Arrangement will have a major impact on both the viability of the information security industry and its ability to protect end-users and corporations via independent and collaborative information security research.

The proposed implementation of the Wassenaar Arrangement will lead to a serious impact on this culture of collaboration that is key to the security industry. Under the proposed implementation the various products that these companies will be working on at any given time will now be subject to the complex and time-laborious process of export control.

At the most basic level we believe that the application of “dual-use” export controls to the tools and work product of security researchers is the incorrect manner to address the concerns of Wassenaar signatories over the development of “0days” or software designed to be used for mass surveillance. Speaking to the specific implementation by BIS we believe that the proposed implementation is overly broad and will go beyond the intent of the wording in the Wassenaar additions, to the point where the proposed implementation may threaten the ability of all but the largest security firms to continue to function as legitimate businesses within the United States. Specifically, the language of “intrusion software” captures a large part of the security community’s endeavors of making systems more secure.

The ability of firms to conduct research and assist US business is critical to the safe and stable running of the US business ecosphere. These firms conduct advanced and specialized research in conjunction with and on behalf of virtually all Fortune 500 businesses and the contribution of

the security testing community is recognized to be a strong force in increasing the security of these businesses. Due to the specialized nature of these businesses many teams are distributed across the globe, recruited from the US, EMEA and APAC. This distributed model has ensured that the availability of top talent to US based businesses has been maintained. Collaboration of research and security investigations across these regions has been paramount to the success of this business model. Being able to start in San Francisco at 8am on a Monday and “follow the sun” across the world on a 24/7 operating schedule is critical in many ways.

Impact

Penetration Testing

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users’ adherence to security policies.

Penetration tests are typically performed using manual or automated technologies to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. Once vulnerabilities have been successfully exploited on a particular system, testers may attempt to use the compromised system to launch subsequent exploits at other internal resources, specifically by trying to incrementally achieve higher levels of security clearance and deeper access to electronic assets and information via privilege escalation.

Information about any security vulnerabilities successfully exploited through penetration testing is typically aggregated and presented to IT and network systems managers to help those professionals make strategic conclusions and prioritize related remediation efforts. The fundamental purpose of penetration testing is to measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.

Penetration testing has become a critical component in every large company’s arsenal of defensive processes. The ability of penetration testers to successfully test against a network’s defenses requires them to be able to utilize advanced tools that would likely come under control via the proposed BIS implementation of the Wassenaar Arrangement.

Red Teams

Red teaming is a multi-discipline, goal-oriented assessment that can last for longer than a couple of weeks. Often nothing is off limits (within reason) but physical, social engineering, etc are all in play for a red team assessment. Also, at least in my experience, there have been more than one person participating on these assessments. There could be specialists from multiple disciplines working in concert to complete the goals. Common goals include gaining specific

pieces of information (such as financial data) from a targeted user's computer, or gaining access to a physical asset and leaving the building with it, or planting a hardware device somewhere on the network.

Defensive Research

Fuzzers are genuine tools which are designed to aid in finding vulnerabilities, which is the first step in producing "intrusion software." As just two examples, Mozilla has a fuzzing system for Firefox, and the Chrome team has their own framework as well. These tools, and others, are used to find and fix vulnerabilities in software, thus making everyone safer. Regulating these tools via export controls would have a serious impact on the products they're helping to improve. ROP Compilers and similar tools are necessary for testing protection mechanisms, but also could be used to create "intrusion software."

Commonly used software is typically developed by companies who operate in multiple countries. To require an export license to send a coworker an update for a tool they need to do their job is an unnecessary burden, which will have an impact on the company's bottom line. This will inevitably result in higher prices to consumers, lost jobs, and/or a decline in the security of the very software people have come to depend on.

The Path Forward

We suggest that the DoC suspends its current implementation of the additions to the Wassenaar Arrangement, we suggest that the GAO is requested to perform an in-depth assessment of the potential impact on the industry paying particular attention to the SME bias of much of the US based security industry, taking into account the various stakeholders at play and their diverse views on the matter.

The security community has shown its willingness to step outside of its traditional technical boundaries and to engage with the USG on this matter, such is its importance to the international security community.

The language of the proposed implementation can then be reassessed with the additional data gleaned from the GAO assessment, ensuring that the needs of the USG to implement the Arrangement do not unnecessarily hinder this most critical of industries.

We believe that a viable solution for both sides may be achieved by pursuing this approach in parallel with an additional, fact-based, drafting round and public comment period in conjunction with the security community.

PUBLIC SUBMISSION

As of: 7/17/15 3:33 PM
Received: July 15, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8jzw-hqho
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0086

Comment on FR Doc # 2015-11642

Submitter Information

Name: Paul Pliska

General Comment

Software should never be subject to export controls. It's been tried before with encryption, and you know what? It was rolled back because it was a TERRIBLE IDEA. And it's still a terrible idea now. It will hurt US businesses and hurt the public.

PUBLIC SUBMISSION

As of: 7/17/15 3:34 PM
Received: July 15, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k00-sosp
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0087

Comment on FR Doc # 2015-11642

Submitter Information

Name: Dale Adams

Address:

2313 Anvil Drive

Harrison, AR, 72601

Email: info@majesticpublishers.com

Phone: 870-365-0827

Fax: 870-365-0827

Organization: Majestic Publishers

General Comment

Hello,

During civil litigation within the United States District Court for the Western District of Arkansas in the civil case Dale Brent Adams v. Tyson Foods, et al., case No. 09-3054, I informed the Judges that oppressive regimes in other countries have also adopted anti-terrorism legislation such as warrantless surveillance and are using these deceptive measures to monitor and oppress political opponents, even with torture.

The United States, formerly a world leader of human rights, free speech with a democracy now has a government that endorses cruel, inhuman degrading treatment and punishment in violation of the Geneva Conventions and is asking for public comments to adopt a treaty where no belief or any information is private, secret or sacred? Even security software?

No person in the world will ever have true liberty by agreeing with this treaty and it is shocking

that our civil government, especially the courts have allowed the military to rule our nation. No person will be safe from oppression and tyranny, including the authors of this treaty.

PUBLIC SUBMISSION

As of: 7/17/15 3:34 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0h-jlka
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0088

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

I am opposed to the proposed rule to subject intrusion and surveillance software to export control. I am not a computer security researcher, but in my role as a Systems Analyst for a local city government, I recognize that vendor-provided security patches are a critical component in keeping our computer systems, and our citizens' data, free and protected from criminal elements.

Many of these vendor security patches are created in direct response to vulnerabilities that are discovered by computer security firms and individual researchers, working all over the world. By closely following computer security news, I can see how these researchers from disparate nations often work together collaboratively, using the Internet as a platform for the free exchange of techniques and ideas.

Legislation and regulation cannot prevent computer intrusion techniques from being discovered, and attack code created and exchanged by those who seek to use them for evil "black hat" purposes. So rather than making the Internet a safer place, the proposed rule implementation would instead make it much more difficult and cumbersome for legitimate and law-abiding "white hat" computer security researchers to do their jobs. This in turn would result in the opposite of what is intended: an Internet that is more dangerous for everyone who uses it.

Thank you for your consideration.

PUBLIC SUBMISSION

As of: 7/17/15 3:35 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0j-2t8b
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0089

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nicholas Weaver

Address:

1947 Center Street Suite 600

Berkeley, CA, 94704

Email: nweaver@icsi.berkeley.edu

Phone: 510-666-2903

General Comment

There appears to be a general belief that the definition of the "surveillance system" is limited in scope. Unfortunately, I do not believe this is the case.

Any modern, scalable Network Intrusion Detection System (NIDS) such as Suricata, Snort, or Bro IDS, is the key component in building a surveillance system, and could potentially fall under the definition of "specially designed" component under ECCN 5A001.j.

A modern NIDS can easily scale to the "backbone" or "carrier" level (there are current NIDS deployments installed on 100 Gbps networks). Thus scale does not distinguish NIDS and IP surveillance systems.

Although NIDS generally don't execute searches on the basis of "hard" or "soft" selectors and/or "map the relationship network", implementing the necessary data gathering for these tasks is simply a small policy script or set of rules in any typical NIDS. I've personally implemented NIDS policy that can identify individuals by extracting usernames from HTTP traffic, which when combined with a user interface to fetch archived traffic, allows direct

attribution of traffic to individuals and would provide the ability to search IP traffic by "hard selectors" in otherwise unstructured network traffic.

Thus it is clear that Network Intrusion Detection Systems are arguably the critical component necessary to build IP surveillance systems, as building the ability to execute hard-selector searches and relationship mapping on top of a NIDS is straightforward.

At the same time, Network Intrusion Detection Systems are a key technology essential for network defense, and any reasonable security posture requires substantial defensive network monitoring. Universities, government offices, and private institutions all rely on NIDS to detect and counter network threats. NIDS is to the network what antivirus is for the end host, a critical component that any network needs to deploy if it wishes to detect and respond to attacks. But with the internal controls and citizenship restrictions under Wassenaar, even internal to the US development and use of NIDS would become effectively impossible, let alone any export of critical defensive security tools.

Thus I believe it is absolutely essential to add an additional exception to ECCN 5A001.j to exclude "Network Intrusion Detection Systems (NIDS)", along with the existing exceptions for Quality of Service, Quality of Experience, and marketing.

This would clearly exempt essential defensive network monitoring tools from the definition of "surveillance systems", and remove the danger of "specially designed" components covering Network Intrusion Detection Systems, while still allowing control of export for true surveillance systems.

Dr Nicholas Weaver, Ph.D.
Researcher, International Computer Science Institute *
(Title for identification purposes only)

PUBLIC SUBMISSION

As of: 7/17/15 3:35 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0l-5p3d
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0090

Comment on FR Doc # 2015-11642

Submitter Information

Name: Kevin Schoonmaker

Address:

331 Kosciuszko St

4R

Brooklyn, NY, 11221

Email: schoonmaker.kevin@gmail.com

Phone: 9179412281

Organization: Domani Studios

General Comment

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

In general, creating a system where licenses have to be granted for in-country transfer and subsequent collaboration on cybersecurity items decreases the speed or probability that cybersecurity researchers will uncover new openings/flaws in contemporary systems.

The black market will continue to function without regard for any import/export restrictions and creating a potential licensing blockade slows the ability for positive countermeasures to be known.

The licensing system for transferring cybersecurity knowledge will also create non-reporters. These are individual hobbyists and researchers who have proven over time to provide valuable

information to US companies and individuals.

If a cybersecurity hobbyist finds valuable information on a cybersecurity flaw they would not be able to report their findings to a company without licensing and would not be inclined to make the information public because they could cause damage. The hobbyist would likely refrain from doing anything and the vulnerability would float until it is taken advantage of by a black market blackhat.

The definition of intrusion software described in section 772.1 is too vague. The software performs The extraction of data or information, from a computer or network-capable device What monitoring tools or protective countermeasures are we defeating and to what extent? The average person transfers much information about themselves unwittingly through internet browser cookies. Are these cookies considered defeating monitoring tools or protective countermeasures? If a cookie is trusted by your Antivirus Software, but not actively by the individual is this an intrusion, extracting data from the individuals browser usage?

If any software used for the development or production of cryptography or cryptographic analysis is controlled, the trial and error process through which a developer creates secure communication platforms is slowed due to the licensing process. In addition, I do not see any laws regulating the timeframe through which licenses will be granted or whether a company/individual can dispute a license denial. There is no guarantee that a company/individual may pursue a needed cybersecurity risk.

In the end, this proposed regulation puts individuals, companies and countries at a slower pace of cybersecurity development with the United States Government being responsible for cybersecurity information dissemination.

Judging from the fact that most publicly known preventative cybersecurity information comes not from the US Government, but from private companies and individuals, I do not believe the US Government has the capability, resources or knowhow to take on this risk.

The intentions of this proposed legislation are good; however, I believe it will have exactly the opposite effect of its intended function.

Black market blackhats will benefit from a slowed, standardized and regulated knowledge pool, putting us all at greater risk and removing faith in the US Government to protect its people.

PUBLIC SUBMISSION

As of: 7/17/15 3:36 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0n-ocxq
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0091

Comment on FR Doc # 2015-11642

Submitter Information

Name: Rolf Rolles

General Comment

Recently, DARPA hosted the Cyber Grand Challenge competition. The participants -- dozens of American companies among them -- were tasked with creating automated systems to find and fix security-related bugs in computer programs. The mission statement for the event was: "Cyber Grand Challenge seeks to someday make software safety the expert domain of machines."

The preeminent technology behind finding bugs in computer programs, known as "automated test-case generation", was created by academic researchers from Stanford, UC Berkeley, Carnegie Mellon, and Microsoft Research, among other institutions. American companies affiliated with these organizations have commercialized the technology and/or put it to use for internal security reasons. ForAllSecure sells a system, Mayhem, allowing customers to find defects in their software automatically. Microsoft regularly touts the successes of their system, SAGE, in securing Microsoft software. Microsoft has recently integrated this technology directly into its Visual Studio 2015 software programming environment, in the form of the "IntelliTest" feature, thus making it available to all programmers everywhere.

On the surface, it seems like a technology that identifies security vulnerabilities for the sake of fixing them should be considered as a defensive one, and hence unrelated to the BIS's current purview. However, the technology previously described as "automated test-case generation" has a second name in the academic research community, which is "automated exploit generation". And on the contrary, that name reads as though it is precisely the type of technology that the

BIS intends to regulate.

The way automated test-case/exploit generation systems find defects in software is by attempting to cause the software to misbehave. To use the more precise language of section 772.1, they attempt to cause "(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions". If successful, they generate artifacts that cause precisely that to happen. The two names for these artifacts, again, are "test cases" (defensive programming terminology) and "exploits" (offensive hacking terminology), and these names mean exactly the same thing in this context.

Hereinlies the problem: the technology itself is neutral, but it can be used for either defensive or offensive purposes. It is a very clear example of dual-use technology. It is already in wide use in a defensive capacity by programmers everywhere making use of the Microsoft Visual Studio IntelliTest feature, ForAllSecure's Mayhem system, or other such systems.

The BIS would do well to ensure that its legislation does not hobble the defensive abilities of software vendors in America and elsewhere to find security vulnerabilities in their products. Doing so would certainly reduce the security of Americans and foreigners, alike and in equal measure. I urge restraint in legislation, and full clarity surrounding issues like these. A second draft and a second round of comments seems warranted, given the delicacy of the circumstances.

Signed,
Rolf Rolles
Mbius Strip Reverse Engineering

PUBLIC SUBMISSION

As of: 7/17/15 3:37 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0o-ma3b
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0092

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

To the Bureau of Industry and Security,

Please reconsider your implementation of the Wassenaar Agreement with regards to the control of intrusion software for research purposes. The agreement states that it controls:

"Information "required for" developing, testing, refining, and evaluating "intrusion software", in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information."

However, I fear that this regulation will cripple the very people who fight against cybercrime. In order to develop countermeasures against the most recent, not-yet-public exploits, researchers would certainly need to have access to the exploits themselves for testing purposes; restricting this access is a terrible misstep.

Imagine trying to train drug-sniffing dogs without samples of the drugs you want to detect. That's what this implementation will do to security experts.

Thanks for your consideration.

PUBLIC SUBMISSION

As of: 7/17/15 3:37 PM
Received: July 16, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k0p-cfgz
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0093

Comment on FR Doc # 2015-11642

Submitter Information

Name: Albert Walton

General Comment

I am not in the computer security business, but the planned rule seems to be a classic case of disarming the good guys while NOT preventing the bad guys from doing whatever they want. The delay required for licensing to communicate about a security problem with a foreign company (or American company with foreign employees) would allow hackers to exploit a newly discovered vulnerability for an extended period of time. Also, the legal uncertainties and red tape will discourage small groups without access to lawyers from participating in security research. To misquote the NRA, "If hacking is outlawed, (or made extremely inconvenient), only outlaws (and the Chinese government) will hack."

PUBLIC SUBMISSION

As of: 7/17/15 3:38 PM
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k10-3a16
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0094

Comment on FR Doc # 2015-11642

Submitter Information

Name: Shad Nygren

General Comment

My comment is that I strongly disagree with this proposed rule. First it seems like you are trying to go back 20 years to the 1990's and the arguments about the legalities around encryption and its export control. I was working in computer IT at the time and remember that like it was yesterday. In the end it was agreed that strong encryption and computer security was essential for business to protect trade secrets from being stolen and securing peoples bank accounts and personal health information etc. This proposal seems like a step back in time that would significantly hinder those legitimate companies based in the USA from helping to secure our critical national infrastructure.

Despite the intentions, this won't protect the United States or its allies from cyber attack. I believe that you are incorrectly categorizing computer bugs and the software used to detect them as "cyber weapons". These are tools - not weapons.

It seems like you had a large team of lawyers, who collectively could not write a single line of computer code, write hundreds of pages of legalese that virtually no computer software person can understand. The result is that legitimate security businesses in the USA will have to hire lawyers and face significant expense in applying for licenses. Smaller organizations and researchers who discover security vulnerabilities but who do not have the resources to hire the attorneys will withhold publication of of critical security vulnerability information.

I am a daily reader of news related to computer security and I use computer security testing

tools on a daily basis to help secure the computing infrastructure for my employer and our customers. Currently I am employed as an IT computer administrator by a company that manufactures smart electric meters which also have the ability to remotely turn off and on electrical power to devices. Therefore, I am one of the computer people who is directly involved in securing what I frequently hear characterized as "critical infrastructure" and this proposed rule threatens to take away a vital source of security information and tools that helps me do my job and keep our critical infrastructure secure. This proposed rule would negatively impact me and many others like me across our nation making us less secure, not more.

This rule reminds me of an ostrich, where the lawyers believe that if they write a hundred pages of rules prohibiting any one from talking about security vulnerabilities and developing security assessment tools, that we can all collectively stick our heads in the sand that the problem will go away. My decades of experience tells me that this is not true. The only way to secure computer networks is to openly discuss the very technical issues involved and then have software developers modify the code to close the vulnerabilities.

I'm also dismayed because if the government spent as much time and effort securing its own infrastructure as it does writing proposed rules precluding computer security discussion like this, that attacks like the recent OPM breach could be prevented. Believe me that this agreement will have zero effect in deterring the criminals and foreign nation states who are probing our computer networks and seeking a way to hack in. They will continue to do what they do. The only thing this agreement will do is make it more difficult for legitimate security researchers and businesses in the USA to help businesses secure their infrastructure from cyber attack.

Please scrap this proposed rule and start over. The focus should be on education and ensuring that organizations make computer security priority #1. In recent hacks security organizations have reported that they are seeing active exploits within hours. Therefore, the focus needs to be on making it easier and faster to disseminate information, tools to identify the vulnerabilities and patches to fix the problems.

I was happy to see that OPM shut down their systems for a few months to perform necessary security upgrades. This is the type of thing that needs to happen and the only way to truly keep hackers out. Organizations that feel that can be secure by outlawing hacking will quickly find that only the outlaws develop hacking tools and communicate with each other about new vulnerabilities. Meanwhile all the white-hats and other security professionals, discouraged by this overburdening legislation, will move on to other fields of work leaving our nations cyber infrastructure increasingly vulnerable and without the knowledge or tools to secure it and in that case the USA would no longer be a cyber leader.

PUBLIC SUBMISSION

As of: 7/17/15 3:39 PM
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k13-79jg
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0095

Comment on FR Doc # 2015-11642

Submitter Information

Name: Cody Curtis

Address:

588 Jackson Street

Amherst, OH, 44001

Email: curtisc89@gmail.com

General Comment

The only thing I can see that this will do is impose more heartaches for the people that aren't out there to do bad things. Black hats/grey hats that are out to profit wont follow any of them as always and the white hats and company owners will just have to go out of their way to become compliant. If anything, I would suggest a bounty system that prevents the desire to try to sell exploits and data and instead makes these people more apt to report these issues to the company owners or some entity designed for accepting and reporting them.

PUBLIC SUBMISSION

As of: 7/17/15 3:40 PM
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-8p3b
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0096

Comment on FR Doc # 2015-11642

Submitter Information

Name: Alan Amesbury

General Comment

Based on my understanding of the proposed rule, it would have serious, adverse impact on my work. I am a security analyst at a major university which has a large, complex, and very open network. I make routine use of tools and software that appear to be covered by the rule, such as tools specifically designed to defeat protective countermeasures of targeted systems and allow for the extration of data or information. I also share information on the behavior of such tools with peers at other institutions, including ones not located within the United States. It is these facts on which I base my belief that the Wassenaar Arrangement, as shown in the Federal Register, would have at minimum an extremely chilling effect on my ability to perform research, collaborate with other researchers, and to perform my basic job functions.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-qtk1
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0097

William Root 6-14-2015

Submitter Information

General Comment

See attached

Attachments

William Root 6-14-2015

June 14, 2015

To: publiccommts@bis.doc.gov

From Bill Root, waroot23@gmail.com, 517 333 8707

Subject Intrusion and Surveillance RIN 0694-AG49

740.2(a)

Permit use of license exceptions for return to the United States under TMP 740.9(a)(14) and APR 740.16 (c, d, e) for all entries in 740.2(a), including proposed (a)(19).

Permit use of license exception TSU operation technology and software 740.13(a) for all entries in 740.2(a), including proposed (a)(19).

Refrain from repeating 740.2(a) prohibitions elsewhere except in special circumstances. Otherwise, the impression is given that, where not done, 740.2(a) is not over-riding. At a minimum, delete proposed revisions of 740.11(a)(2)(vi) and 740.11(c)(3)(viii) unless the same is done for 740.11(d)(2)(iv). Preferably, delete 740.11(a)(2)(vi) and 740.11(c)(3)(viii) unless the same is done for all the following, not only for (a)(19) but also for all the other 740.2(a) prohibitions (where possible, simply add a new subparagraph, *e.g.*, (D) following 740.9(b)(1)(iii)(C); otherwise, entry is marked “exception”):

740.9(b)(1)(iii)(D)
740.9(b)(1)(iv)(D)
740.9(b)(2)(iii)(D)
740.9(b)(3) exception

740.10(a)(3)(ix)
740.10(b)(1) exception
740.10(b)(2) exception
740.10(b)(3)(i)(G)

740.11(d)(2)(iv)

740.13(a)(2)(i)(C)
740.13(b)(2)(i)(C)
740.13(c) exception

740.14(c)(5)

740.15(b) exception
740.15(c) exception

740.16(b)(1) exception

740.16(f) exception
740.16(h) exception

740.17 exception

746.2(a)(1) Cuban embargo license exceptions
746.3(c) Iraq embargo license exceptions
746.4(c) North Korean embargo license exceptions
746.6(c) Crimean embargo license exceptions
746.9(b) Syrian embargo license exceptions

742.6(b)

Move licensing policy to governments of Australia, New Zealand, and United Kingdom to a separate sentence, in order to show favorable treatment pursuant to partnership with United States (omit Canada, because of no license requirement to Canada for these items). Reflecting such international agreements in the EAR is a major positive step.

The special treatment to the United Kingdom and Australia (and Canada, where applicable), under broader treaties with those countries for munitions items, should also be reflected in EAR license requirements for “600 series” and “500 series” ECCNs.

NP

Remove NP from 4A001 and 4A003
(For same reasons proposal removes NP from 4D001 and 4E001.)

Other Technical Corrections

After “5B001.a” insert “for 5A001.j” in:

740.2(a)(19) three times
740.11(a)(2)(vi) three times
740.11(c)(3)(viii) two times
740.13(d)(2)(ii)
740.17
740.20(b)(2)(ix) three times
742.6(b)(5) three times
748 Supplement 2(z) three times
5D001 RS applies
5D001 License Requirement Note
5E001 License Requirement Note
5E001 Related Controls
5E001 TSR
5D002 Related Controls

4A005 Related Controls (2) change XIII to XIII(b)

4D001 Related Controls after USML add XI(d) for XI(b) and XIII(l) for XIII(b)

4E001 RS applies change “and if “required” for 4E001.c” to “and to 4E001.c”

4E001 License Requirement Note change “if required for 4E001.c” to “for 4E001.c”

4E001 STA change “4D004), 4D004” to “4D004) or 4D004”

5A001 Related Controls (5) add 2A984

5D001 TSR change “and 5A001.j” to “or 5A001.j”

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-desu
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0098

Watson Ladd 5-20-2015

Submitter Information

General Comment

See attached

Attachments

Watson Ladd 5-20-2015

Sharron Cook

From: Watson Ladd <watsonbladd@gmail.com>
Sent: Wednesday, May 20, 2015 10:36 AM
To: PublicComments
Subject: RIN 0694-AG49

To whom it may concern,

My name is Watson Ladd, and I am a graduate student at UC Berkeley studying number theory and cryptography. I also routinely find bugs in open-source and other programs, some of which have security implications and get them fixed. The proposed rules would hamper my ability to communicate security bugs to vendors and get them fixed effectively, as well as to develop defenses to exploitation.

The most effective way to demonstrate that a bug exists and is serious, is to demonstrate a proof of concept, an input which exploits the bug. This code could easily be modified to have a malicious payload. Banning its export would make it impossible in some cases to convince recalcitrant vendors of the reality of this issue, if the vendor is overseas.

Developing defensive measures against exploitation depends on understanding how exploitation works in practice. This requires public knowledge of the means by which bugs may be turned into exploits. For example, phrack's article on the Malloc Maleficarum prompted new designs for memory allocators that lack the data structures which are exploited. Later articles on bypassing these new protections lead to more enhancements, increasing security. Attackers already know all the tricks, and it is unclear how far "technology" goes: are conference papers containing exploit code technology for creating intrusion software?

Even if these rules are not intended to have such effects, the existence of these rules may cause firms and individuals to err away from these valuable activities for fear of violating these rules. The expense of legal advice will further deter independent research and publication in this area.

I propose adding license exceptions for disclosure of bugs and PoC code to vendors or to the public, and the public discussion of offensive methods, so as to make clear that these modifications to the export control rules are not intended to affect widespread practices in the security industry today. I feel that these exceptions are limited in scope, protect valuable activities, and do not weaken prohibitions against actions that should be prohibited.

Thank you for your time.

Sincerely,
Watson Ladd

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-k2zm
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0099

Scott Francis 5-20-2015

Submitter Information

General Comment

See attached

Attachments

Scott Francis 5-20-2015

Sharron Cook

From: Scott Francis <darkuncle@darkuncle.net>
Sent: Wednesday, May 20, 2015 2:59 PM
To: PublicComments
Subject: Re: BIS-2015-0011

I am strongly opposed to the proposed rulemaking (classification of vulnerability research tools as export-controlled), for several reasons:

1) software is not a weapon, nor is it dual-use. The original WA finding that led to the 2013 decision to classify vulnerability research tools (incorrectly referred to as "intrusion software" in the rulemaking) needs to be revisited, with deference given to input from technical experts who actually understand the items which face regulation. The rulemaking, as it now stands, is replete with inaccuracies and misunderstandings as relate to these tools and security research in general.

2) the proposed regulation would not actually achieve its stated goals: as with the development of cryptography in the 1990s, all this will accomplish is to move research offshore, putting the United States and other WA signatories at a disadvantage and encouraging talented researchers who might otherwise be available to US companies and agencies to avoid them.

The design and practical effect of the Internet is specifically to route around this kind of restriction, enabling people to continue to collaborate and share ideas by avoiding meddlesome local regulations. For example, China's restrictions on discussion or reference to Tiananmen Square have not erased such things from the Internet; discussion goes on and information remains available by simply avoiding Chinese restrictions. Development on advanced cryptography and security protocols in the OpenBSD project continued throughout the 90s, despite US export restrictions on crypto, by moving the project source code repository and primary developers outside the US.

Many of the most well-known and effective security research tools that would fall under this proposed rulemaking are open-source tools developed by thousands of people around the world, collaborating over the Internet: geographic-based restrictions on export and control are ineffective here, because there's no single entity to license (the code is freely available, and can be - and already is being - copied an infinite number of times, to millions of locations worldwide). At its core, computer source code is mathematics - and mathematics are just ideas, that defy restriction.

This kind of regulation only serves to put a damper on the creativity (and civil liberties) of brilliant US researchers - the same creativity which is a primary engine of business and economic growth.

3) besides being technically incorrect and practically ineffective, such regulation puts a strong "chilling effect" on critical, beneficial security research that might be related to or leverage "intrusion software" - the kind of security research that is DESPERATELY needed to help keep the US and US companies secure against an unending string of ever-improving attacks from external state actors and criminal enterprises who are not bound by these same regulations.

The high-profile attacks on Google, RSA, Microsoft, major defense contractors and virtually all major US federal agencies underscore how critical it is to actively promote a strong, healthy security research community here in the US: to protect vital infrastructure, the competitive advantage built up by US businesses, our national security interests, and the private information of millions of US citizens. The threat landscape on the Internet is constantly evolving, and if we voluntarily remove ourselves from that evolution by declaring it illegal, we will only make ourselves increasingly vulnerable to those who continue to move on.

4) this rulemaking is contrary to core US values of civil liberties and free speech - computer source code is speech, not a weapon to be regulated (e.g. by ITAR), as recognized by the 9th Circuit in *Bernstein v. DOJ* (see <https://www.eff.org/cases/bernstein-v-us-dept-justice>). Besides being a self-inflicted harm, ineffective in practice and based on a wholly flawed understanding of the underlying technologies, this regulation is unconstitutional and un-American: we value liberty and free speech, and place restrictions on those only with overwhelming good cause, which is not present here.

5) this rulemaking would harm US companies that work internationally or offer services over the Internet to international clients, as well as US divisions of international companies - the uncertainty and confusion introduced here, especially to corporations whose business is information security, would be crippling (as would the associated legal fees and time lost trying to determine compliance). As with item (2), this would only serve to put the US as a distinct disadvantage (in both security posture and business competitiveness) to the rest of the world.

sincerely,
Scott Francis

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-8tfs
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0100

Richard Bradley 5-22-15

Submitter Information

General Comment

See attached

Attachments

Richard Bradley 5-22-15

Sharron Cook

From: Richards Bradley <bradley.richards@fhnw.ch>
Sent: Friday, May 22, 2015 2:33 AM
To: PublicComments
Subject: Comment on BIS-2015-0011

Ladies and gentlemen

Rule BIS-2015-0011 is essentially proposing export restrictions on information. While it may refer to software products, in fact, there is no practical difference between controlling software and controlling the concepts that it implements: given the concepts, anyone can write the software.

This rule is reminiscent of the one-time export controls on cryptographic products. This proposed rule would be counterproductive, just as those export controls were. In fact, we are still paying the price of those one-time export controls: just this month, a widespread security problem ("Logjam") was identified, which can be directly blamed on those futile attempts to control encryption technology.

Rules like this are proposed by well-meaning but arrogant government agencies. You presume much more power and control than you actually have. In today's society, no one can control the flow of information in this way (or, indeed, in any realistic way). All that such rules accomplish is to hamper law-abiding companies and individuals, thereby benefiting illegal actors.

Rule BIS-2015-0011 is a bad idea. Scrap it.

Yours sincerely

Dr. Brad Richards
Professor of Computer Science
Switzerland

Fachhochschule Nordwestschweiz FHNW
Hochschule für Wirtschaft
Institut für Wirtschaftsinformatik

Prof. Dr. Bradley Richards
Riggenbachstrasse 16, CH-4600 Olten
T +41 62 957 2387
M +41-79-598-6331
bradley.richards@fhnw.ch
<http://www.fhnw.ch/wirtschaft>

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-ynbx
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0101

Raytheon BIS Cybersecurity Rule - Extension Request 7-10-15

Submitter Information

General Comment

See attached

Attachments

Raytheon BIS Cybersecurity Rule - Extension Request 7-10-15

July 10, 2015

Via Email

Regulatory Policy Division
Bureau of Industry and Security (BIS)
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. N.W.
Washington, DC 20230

Email: publiccomments@bis.doc.gov

Reference: RIN 0694–AG49

Subject: Request for Extension of Deadline for Submission of Comments Regarding
Proposed Cybersecurity Rule

To Whom It May Concern:

Raytheon Company (“Raytheon”) requests an extension of the deadline to file comments to the Bureau of Industry and Security (“BIS”) in response to the Proposed Rule implementing the Wassenaar Arrangement’s 2013 Plenary Agreements on intrusion and surveillance items (80 Fed. Reg. 28,853, May 20, 2015).

This proposed rule would have a sweeping impact on the cybersecurity industry, including many of Raytheon’s business activities, and given the breadth and depth of Raytheon’s work in this area, it will not be feasible for the company to provide meaningful and helpful comments to BIS by the current deadline of July 20, 2015. Raytheon requires more time to be able to consider the potentially very significant impact of this rule across its businesses, particularly in light of the complicated nature of the proposed rule, as well as the summer vacation schedules of the many company personnel whose input is critical to allowing Raytheon to provide thoughtful feedback to BIS.

Therefore, we respectfully request that BIS extend the comment deadline by an additional 60 days.

RIN 0694-AG49

July 10, 2015

Page 2

If you have any questions concerning this submission, please contact the undersigned at julia.court.ryan@raytheon.com or (703) 284-4459; karl.abendschein@raytheon.com or (703) 284-4275.

Sincerely,



Julia Court Ryan
Senior Counsel
Global Trade Compliance, Governance

Karl Abendschein
Senior Manager
Global Trade Compliance, Governance

cc: Hillary Hess, Kevin Wolf, Catherine Wheeler

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k17-wxnj
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0102

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

I work in the field of Information Security at the University of Minnesota. The regulations proposed here would drastically impact my ability to perform my job duties. By placing restrictions on software that can be used for intrusive purposes, you limit security researchers abilities to offensively test their own systems for vulnerabilities. There are countless tools that are used in these offensive "penetration tests" that would be restricted under this proposal. I can name over a hundred specific examples (any tool included in Kali Linux), but for brevity's sake I will refrain from listing all the tools that this regulation would impact.

I urge you to listen to the advice of us who are working to protect technology. While it might seem counter-intuitive, limiting the sharing of intrusion oriented programs and information only hinders those of us who operate within the bounds of the law. Those who seek to violate the law will continue to do so, while those of us who seek to defend will no longer be able to identify security holes in our environments.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k18-p1xc
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0103

Justin Yakoski 6-16-2015

Submitter Information

General Comment

See attached

Attachments

Justin Yakoski 6-16-2015

Sharron Cook

From: Justin Yackoski <jyackoski@i-a-i.com>
Sent: Tuesday, June 16, 2015 5:13 PM
To: PublicComments
Subject: comments on BIS-2015-0011

I would like to submit comments in regard to proposed rule BIS-2015-0011, "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items".

As someone involved in advanced cyber security research at a company that has significant work with the US government and DoD, we are forced to be very risk averse and error on the side of following the law whenever ANY question or doubt exists. This type of situation already comes up almost constantly, and the answer/conclusion we reach is that we should avoid anything that potentially exposes us to any risk. I think this is the only reasonable conclusion.

Due to the extremely broad and unclear nature of the proposed rule, I am absolutely certain that it will be interpreted and result in corporate policies throughout the community that error on the side of low risk. This necessary interpretation by the people affected by the rule will unequivocally place a significant burden on future development efforts. It will make finding appropriately skilled staff much more complex, working efficiently much more elusive, and sharing results/data/technology almost impossible.

If the intended effect of the rule is to completely stifle security related technology development in the US at a time when other countries are greatly accelerating their cyber security capabilities to use against us, then this is a perfectly designed rule. The government and commercial cyber security worlds will be further pushed apart to the point where government-affiliated cyber security work becomes impossible and commercial work becomes highly secretive and barely profitable.

Please clarify the rule to very clearly impose what the rule is intended to cover. If you make a rule from an ivory tower without any consideration of the practical effects (which seems very much to be the case here), then there will be severe unintended negative consequences on people like me on a daily basis.

Thank you.

Justin

--

Justin Yackoski, Ph.D.

Program Manager

Intelligent Automation, Inc.

15400 Calhoun Drive, Suite 190

Rockville, MD 20855

<http://www.i-a-i.com>

Email : jyackoski@i-a-i.com

Direct: (301) 294-4251

This message and all attachments are PRIVATE, and contain information that is PROPRIETARY to Intelligent Automation, Inc. You are not authorized to transmit or otherwise disclose this message or any attachments to any third party whatsoever without the express written consent of Intelligent Automation, Inc. If you received this message in error or you are not willing to view this message or any attachments on a confidential basis, please immediately delete this email and any attachments and notify Intelligent Automation, Inc.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 17, 2015
Tracking No. 1jz-8k18-5dzb
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0104

David Wilburn 7-16-2015

Submitter Information

General Comment

See attached

Attachments

David Wilburn 7-16-2015

Sharron Cook

From: David Wilburn <david.m.wilburn@gmail.com>
Sent: Thursday, July 16, 2015 9:33 PM
To: PublicComments
Subject: Public comments to RIN 0694-AG49 (proposed rulemaking related to Wassenaar Arrangement)

16 June 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

To whom it may concern,

On behalf of David Wilburn and Ben Schmoker, we are writing in regards to proposed rulemaking published in the federal register with the ID BIS-2015-0011 and RIN 0694-AG49, available at:

<https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>.

This proposed rulemaking is intended to update the United States Government's implementation of the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.

While we write as concerned citizens, we are also professional cyber security engineers with cumulative decades of experience. We lead teams of fellow cyber security engineers in researching and developing new solutions to defend the networks of the United States Department of Defense and civilian departments and agencies from Advanced Persistent Threat actors. Our published work includes threat intelligence and mobile security in such venues as DFRWS (Digital Forensics Research Workshop) and IEEE (Institute of Electrical and Electronics Engineers).

The proposed rulemaking is well-intentioned, and may yet provide some benefits. Sale and distribution of surveillance tools to repressive regimes is deeply troubling, as is their apparent use to stifle dissenting opinion and enable crimes against humanity.

Recent examples of companies that have sold surveillance tools to repressive regimes include Hacking Team via the RCS tool, Gamma Group's FinFisher product, and at least indirectly, Blue Coat Systems' web filtering appliance. Reports from Citizen Lab (<https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/>) and Reporters Without Borders (<http://surveillance.rsf.org/en/category/corporate-enemies/>) on this subject make for compelling reading. It is comforting to know that the US Government and our allies take these issues seriously. However, the benefits from the

proposed rulemaking are unlikely to prevent bad actors from possessing and abusing security tools with potential surveillance capabilities, while likely creating significant problems for US interests.

The ethical nature of technology this proposed rulemaking seeks to regulate is largely neutral. Its abuse can be characterized by bad intent combined with questionable or nonexistent legal authority, and whether express consent of affected parties was given. However, the proposed rulemaking provides very little room for the distribution of regulated technology with benign intent.

Defensive technologies work in a technical manner similar or identical to surveillance software. Such defensive technologies include, but may not be limited to:

- * Data Loss Prevention tools,
- * Insider threat monitoring tools,
- * Digital forensics tools,
- * Vulnerability assessment tools,
- * Penetration testing tools,
- * Deep Packet Inspection (DPI) technologies,
- * Remote administration tools, and
- * Traffic inspection technologies.

Each of these technologies operate through passively monitoring network traffic, actively manipulating network traffic, injecting code into processes on host systems, and/or hiding their presence. These are all functionally similar or identical to the technologies that the proposed rulemaking intends to restrict.

Critical tools that are broadly available to network defenders today would become heavily restricted or unavailable under these proposed rules. Again, the only substantial difference is the intent. Individuals and businesses who develop and sell such tools will be exposed to significant risk in continuing to develop and distribute their technologies. Many developers or vendors of these defensive technologies may feel forced to erect barriers to acquiring their technologies, even for domestic audiences, out of an abundance of caution. Others may choose to withdraw from the cyber security market rather than face new bureaucratic challenges and legal risks. In the event that security tool developers withdraw from the market, this will effectively deprive the US and its allies of valuable defensive technologies, and cause it to lose valuable mindshare.

Much of the proposed rulemaking is ambiguous and vague, and nearly impossible for an expert in the art of cyber security to interpret. This will create a significant burden on the information security industry to acquaint itself with new rules, seek legal advice, and retrain an enormous cyber security workforce. Worse, the proposed rulemaking leaves significant gaps to be addressed (or not) by the Department of Commerce at a later, unspecified date. While the proposed rulemaking provides a vague statement that, "BIS anticipates licensing broad authorizations to certain types of end users and destinations", it is impossible to fully interpret the potential negative impact to the cyber security industry until these broad authorizations, types of end users, and destinations are actually defined. It also leaves room for the BIS to put off such authorizations indefinitely, or define the types of users and destinations very narrowly. Even if the enforcement of this proposed rulemaking is very conservative, it will be very prone to abuse through selective enforcement. Ambiguous rules backed with the force of law are anathema to good governance and equal protection.

While it may be tempting to view the proposed rulemaking as only affecting international commerce, the reality is likely to be much more complex. The global nature of the Internet, which serves as the primary means of distributing technologies covered under the proposed rulemaking, means that it is very difficult to restrict technologies to domestic audiences or specific countries. Common security controls and restrictions used for this purpose, such as geolocation of network traffic are broadly considered weak and easily bypassed. Affected parties may feel compelled to withdraw from timely distribution of critical technologies via the Internet, due to the ambiguities. This will have enormous effects on the domestic security industry, rather than just repressive regimes. These rules might cause the operators of Internet-based mailing lists, chat channels, web forums, FTP servers, content delivery networks, mirrors, hosting providers, operating system distributors, software vendors, resellers, and legitimate peer-to-peer distribution mechanisms to create onerous restrictions in an attempt to comply, or close down altogether. Domestic audiences of security tools may find themselves unable to reasonably acquire tools and knowledge from even domestic suppliers.

The US government, as one of the largest single purchasers of information security and cyber security technology, is likely to be affected negatively, as well. It will suffer from the same overall market hesitations and withdrawals as other parties. It will also suffer uniquely, in greater difficulty posed to supporting its international obligations. This includes support to NATO, member nations, and other allies with cyber security technologies. It also includes support to partner nations and other countries with emerging US interests. Additionally, it includes support to the US military stationed abroad and US missions, whose US civilian or contractor workforces may find it difficult or impossible to provide security solutions. It is worth noting that a substantial portion of the US military's overseas networks are defended by US-based or multinational contractors, and the BIS's proposed rulemaking would explicitly prohibit transferring needed technologies without a license. If the Department of Commerce carries out this proposed rulemaking, then it will likely be placing itself between the US Departments of Defense and State, and America's allies. Given the increasing global threat from cyberattack and cyberespionage, this would seem unwise.

The proposed rulemaking is likely to inhibit cyber threat intelligence analysts, malware analysts, vulnerability researchers, and other cyber security professionals on a daily basis. Modern security operations depend upon the timely receipt and processing of malware, vulnerability research, cyber threat indicators, and other tools and information. For instance, this rulemaking is likely to inhibit or destroy existing collaborative efforts and resources, such as Virus Share and Virus Total, because it will make the legality of sharing of malware samples dangerously ambiguous. These resources exist to serve network defenders and security researchers, rather than malware authors or other ne'er-do-wells. Without the ability to easily share and analyze emerging threats, including malware samples, network defenders will be left deprived of valuable cyber threat intelligence. The explicit exemptions for reverse engineering tools are necessary, but not sufficient, if the malware samples, exploit tools, and vulnerability research cannot be rapidly shared within responsible circles.

Even if the BIS prioritizes the processing of applications for exemptions under this proposed rule, it is extremely unlikely to be timely for its purpose. The dissemination of vulnerability information and cyber threat intelligence is time-critical. Any friction added to this environment, even by an eagerly supportive bureaucracy, is likely to significantly diminish the value of this information.

The proposed rulemaking is likely to heavily impact vulnerability research and penetration testing. In these fields, it is accepted practice to include proof-of-concept exploit code to enable further analysis and discussion, but the proposed rulemaking would make such research legally dangerous. The process for seeking exemptions for these are largely undefined. This will have the effect of driving vulnerability researchers and penetration testers away from their field, or underground. The eventual effect is that vulnerable infrastructure will remain undetected by network defenders, while adversaries will have little such restrictions.

Additionally, these restrictions are likely to deprive the US of its full ability to recruit and train the cyber workforce that it desperately needs. Universities may find the teaching of covered technologies to no longer be worth the risk, especially when so many students come from abroad. Less formal instruction and information sharing through security conferences, private training programs, and local hackerspaces, will also be negatively affected. It is also worth noting that modern cyber security professionals find Capture The Flag (CTF) programs to be extremely valuable in building and testing their security skills. In CTF programs, security students and professionals learn to defend and attack networks in controlled environments. However, under the proposed rulemaking, CTF organizers may find it simply too risky. This will reduce the quantity and quality of security professionals within the US workforce.

Crucially, the parts of the world that create the greatest concern for creation, distribution, and misuse of malware, are extremely unlikely to be affected. While Russia is a signatory to the Wassenaar Agreement, it is also a significant adversary of the US in cyberspace, and has repeatedly shown itself to be unwilling or unable to exercise or enforce restraint in cyber-crime and cyber-espionage that is directed towards American interests. China, who has consistently acted with hostility towards the US government and industry in cyber-crime and cyber-espionage, is not even a signatory. Both Russia and China are notorious for their black market cyber-crime activity, which is rarely punished as long as the crime is directed towards Western interests. These two countries are also significant sources of assistance to a broad range of repressive regimes, and it is very likely that they will fill in any gaps created by the updated Wassenaar Agreement. American diplomacy has historically proven unable to rein in hostile activity in undesirable trade and other forms of support by Russia and China to repressive regimes, and nothing in this updated agreement is likely to change that. It is therefore very unlikely that the Wassenaar Agreement will have the intended effect of significantly limiting critical cyber security tools to repressive regimes.

It is also worth noting that the US government's role in the global market of hacking tools has not been altogether positive. There are strong indications that the US government, supported by the defense industry, is one of the top buyers for 0-day exploit code on the commercial market, as indicated in the 2012 Forbes Article, Shopping For Zero-Days: A Price List For Exploits. Recent public disclosures regarding the Italian firm Hacking Team indicate that multiple US government agencies have purchased surveillance tools alongside repressive regimes. America and her allies, including other signatories of the Wassenaar Arrangement, have often been enthusiastic adopters in very controversial circumstances of the very technologies that this rulemaking is intended to restrict. Absent comprehensive and transparent reform amongst the signatories, including the US government, this rulemaking is likely to be viewed as deeply cynical and hypocritical by Americans and peoples across the world.

Perhaps most ironically, while the proposed rules seek to restrict the availability of exploit tools, they do absolutely nothing to address the continued availability and distribution of vulnerable information technology of extremely shoddy quality. This discussion only exists because the current state of the software market supports poorly designed and implemented software, which is routinely shipped to domestic and foreign users full of undiscovered vulnerabilities. The overall effect would be to turn a blind eye to vulnerable software, while threatening security researchers and professionals who might point out exploitable vulnerabilities within them. This will have a chilling effect on free speech, and result in an overall loss in real security.

BIS has taken some commendable steps in developing a FAQ to address concerns from the public. However, it is unclear whether the clarifications BIS provides in a FAQ on their website will carry the same weight as the published regulations, or whether they might be prone to change. We would strongly recommend that substantial clarifications be rolled back into the regulation itself. Additionally, the current clarifications leave several remaining concerns.

The BIS FAQ makes it fairly clear that open source technologies and openly published information is exempt from the controls. While this is an excellent exemption, it does not fully address the concerns. Full disclosure remains a common, but controversial model for vulnerability disclosure. It is often the preferred model when software vendors are uncooperative or dismissive of reported vulnerabilities, but is not always desirable in the general case. Full publication of detailed vulnerability and exploitation information to the public writ large is often considered irresponsible, especially before the vendor has been given a chance to develop, test, and distribute a fix. While the security industry has not established clear standards in this area, much of the security community has gravitated towards responsible vulnerability disclosure, perhaps best outlined in the draft IETF standard “Responsible Vulnerability Disclosure Process” (Christy, S., Wysopal, C., 2002). In the field of responsible vulnerability disclosure, it is customary to provide a security vendor with detailed exploitation information in confidence. This information may also optionally be relayed through an independent vulnerability coordinator, such as SEI/CERT. The detailed information often includes “technical data to create a controllable exploit” that BIS asserts would be controlled under this rulemaking. This would effectively discourage or delay responsible vulnerability disclosure, in the event that one or more parties cross international borders or may not be US citizens. Conversely, it may also inadvertently encourage the most irresponsible forms of full disclosure without any opportunity for security vendor patching, because full disclosure would be uncontrolled under the proposed rulemaking. It is unclear why BIS would desire to discourage responsible vulnerability disclosure, while encouraging irresponsible practices. The manner in which vulnerabilities are disclosed, and how openly and fully their details are exposed to the public, should be chosen by the vulnerability researchers most familiar with the potential consequences. BIS should make an explicit blanket exception for responsible vulnerability disclosure that involves otherwise controlled information.

The BIS rulemaking and associated FAQ are unclear in their definitions of intrusion software. The FAQ attempts to provide some clarification repeatedly, but the clarifications are unclear to experts in the art. The attempts at distinguishing between covered intrusion software and uncovered exploits and malware appear to offer a distinction without a difference. It is also unclear why the BIS would wish to control software that modifies execution paths, but freely allow exported software that is destructive in nature. There are also some chicken-and-egg problems, such as the fact that supposedly uncovered proof-of-concept exploits cannot technically function without modifying execution paths, which is explicitly covered by the proposed rulemaking. Whole classes of vulnerabilities, such as buffer overflows, would therefore likely be covered by the proposed rulemaking, despite BIS’s assertions to the contrary. It is further unclear how BIS would expect vulnerability research to be conducted when it allows some technologies (e.g., reverse engineering tools, fuzzers, etc.), while denying other critical technologies without a license (e.g., technology required for the development of intrusion software), or how such controlled and uncontrolled technologies could be reliably distinguished from each other by an expert in the art. Further, the proposed rulemaking would tend to stifle vulnerability research into network-enabled software such as client and server software, because the natural path of execution would inherently include communication with intrusion software.

The BIS rulemaking appears to allow vulnerability research against traditional software applications, but the explicit restrictions on software that defeats “protective countermeasures” would appear to effectively ban some forms of vulnerability research against security applications. Due to their special role, security applications deserve even greater scrutiny than traditional software, and BIS should alter or clarify the controls of software that defeats protective countermeasures to explicitly allow such work to be freely conducted. There are already some indications that the United Kingdom’s rulemaking related to Wassenaar has stifled such research, including research into the effectiveness of EMET (Willcox, G., 2015). It would be a shame if BIS did not learn from the mistakes of other signatories to Wassenaar, and created an environment in the US that discourages valid research into the vulnerabilities and effectiveness of security tools. Otherwise, we may be left with snake oil being sold as security, with decreased opportunity for independent evaluation.

With regard to your questions in the federal register:

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

a. How many additional applications would be for products that are currently eligible for license exceptions?

b. How many additional applications would be for products that currently are classified EAR99?

Without providing binding advice, these rules appear to require submission of multiple license applications per year for a domestic US company with any international presence. This includes especially defense contractors that provide cyber security support to the US military overseas. The number of such applications would depend greatly on the nature of the work, as well as the specific procedures that the Department of Commerce creates, such as how broad the exemptions might be.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

Same answer as above.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

Yes, it almost certainly would have negative effects. It would make the rules regarding publication of vulnerability research ambiguous. It would make acquisition of defensive tools, including but not limited to vulnerability assessment and penetration testing tools, more difficult, and would likely reduce the overall availability of them. It would tend to make sharing of malware samples within collaborative environments very difficult for network defenders, resulting in lack of timely cyber threat intelligence for network defense. It would tend to restrict the availability and use of network and host security monitoring tools for detection and response. It would make security support to the US military, NATO, and other international interests of the US much more difficult.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

We are unable to clearly determine the applicable requirements, or a reasonable amount of time that would be required to fulfill them. The Department of Commerce should seek to create rules that are unambiguous and easy to follow for practitioners in the art.

Based on these concerns, we strongly urge the Department of Commerce to withdraw its proposed rulemaking. While well-intentioned, it is more likely to do harm to our national interests than benefit them. Additionally, it is very likely to stifle domestic innovation in the field of cyber security, by discouraging security research and commerce. If the Department of Commerce intends to continue forward, we strongly recommend adopting broad exemptions. In particular, restrictions and enforcement should only be imposed when the government can prove malicious intent, such as actively marketing covered technologies to repressive regimes knowing their likely repressive purpose, or developing or distributing malware for the intended purpose of enabling cyber-crime. It is excellent that broad exemptions have

been put in place for technology that is open source. However, further broad exemptions should be enacted for collaborative forums that are predominantly serving security researchers and network defenders, and security work that occurs in confidence rather than fully in the public. These restrictions should be proactively defined on an umbrella basis, rather than requiring individual applications by security researchers and professionals that may lack the expensive legal expertise required to navigate through this process.

Sincerely,

David Wilburn

Ben Schmoker

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 17, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k18-o6vd
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0105

Comment on FR Doc # 2015-11642

Submitter Information

Name: Christopher Carlson

Address:

49002

Email: c.s.carlson6@gmail.com

General Comment

Dear BIS investigators,

My name is Chris Carlson, I am a computer scientist and a small business owner from Michigan, and I am writing to encourage you to reconsider some particularly troubling wording in this proposed regulation. I am also requesting that you create at least one more draft and open it up for comments before finalizing any rules or regulations. This issue is a complex one and needs to be considered carefully before making any changes, and while I understand the motivation for the regulation, I none-the-less implore you to remain calm and take your time in drafting it.

Recognize first that the state of the internet is and has been relatively insecure for many years now, and that even though the revelations brought about by the hacking of Hacking Team and the subsequent release of their data is troubling, the digital landscape hasn't actually changed at all.

Realize also that most security researchers in America and abroad are working tirelessly to uncover security flaws in our own infrastructure and in the systems we run. The people working on these things should be taken very seriously when they recommend against a proposed rule.

These people know what will make their jobs harder and what will make their jobs easier. Because their job is keeping American Citizens computers safe from hackers, you should do anything and everything you can to help them achieve that goal.

In this instance the particular wording of "Intrusion Software" is problematic. It is defined too broadly, as a computer scientist and small business owner I agree with this statement. Intrusion Software is currently defined as, software that is capable of extracting or modifying data or modifying the standard execution path of software in order to allow the execution of externally provided instructions. This definition is frightening to me in many ways. It's quite vague and could easily apply to many security programs one might use to diagnose or repair an infected computer. It could also easily apply to any number of service based programs one might write into a secure networking program. Even as a person who's business focus is not particularly on security, I would have a harder time knowing if my products were legal to publish based on this definition.

I recommend you look into the proposal by Professor Sergey Bratus of Dartmouth College. His suggestion of focusing on the act of stealing data is a much better solution for this particular problem. It won't hinder software developers, computer scientists, or security researchers from doing their jobs, but it does address the issue of theft of data which is what you want.

Thank you sincerely for your time, I appreciate you taking my comments into consideration.

-Christopher Carlson

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k24-q3nm
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0106

Comment on FR Doc # 2015-11642

Submitter Information

Name: Martin Peck

Address:

27464 SW Vanderschuer Rd
Hillsboro, OR, 97123

Email: coderman@gmail.com

General Comment

Where as diplomatic agreements compel compliance with the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013, let it be understood that "intrusion software" as a concept attempts to govern thoughts of users of general purpose computing machines.

Where as governing the thoughts of humanity is foolish, using their actions as guide to their intent results in better guidance.

Therefore, compliance without undue restraint demands that only activities of covert intrusion be penalized, and all software must remain outside realm of control of BIS.

Finally, in the spirit of reducing harm, as Wassenaar Arrangement nobly attempted but failed horribly, BIS must rule anything but #FullDisclosure of vulnerabilities as aiding violations against basic human rights. There is no perfect control over information, thus anything less than #FullDisclosure is aiding unknowns with access to early notification of defects in industry.

Thank you for your consideration.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k27-ahr4
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0107

Comment on FR Doc # 2015-11642

Submitter Information

Name: Richard Salz

Address:

Akamai Technologies
150 Broadway
Cambridge, MA, 02142

Email: rsalz@akamai.com

Phone: 781-789-3974

General Comment

The items are so poorly defined that they will stifle research and prevent good things from being done. Do not adopt this!

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2f-3ji6
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0108

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matthew Goldstein

Address:

1012 14th Street NW Suite 620

Washington, DC, 20005

Email: matthew@goldsteinpllc.com

Phone: 202-550-0040

General Comment

See attached file(s)

Attachments

GPLLC Comment Cyber Rule 19July2015

RE: RIN 0694–AG49
BIS-2015-0011

July 19, 2015

PUBLIC COMMENT

This is a public comment to RIN 0694–AG49, as published by the Department of Commerce Bureau of Industry and Security (“BIS”) at 80 Fed. Reg. 28,853 (May 20, 2015) (the “Proposed Rule”), titled, “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items.”

According to the latest forecast from Gartner, Inc. (NYSE: IT), worldwide spending on information security will grow 8.2 percent in 2015 to reach \$76.9 billion.

U.S. companies rely on cybersecurity tools and technology to protect their corporate resources and information. Cybersecurity professionals are hired to find vulnerabilities in networks and exercise a company’s ability to detect and respond to a cyber attack. Both of these tasks require access to technologies BIS seeks to control in the Proposed Rule.

Although the Proposed Rule is published with good intentions, it will significantly impede the ability of cybersecurity professionals to protect multinational company computer systems and networks because it will remove well-established license exceptions that currently allow cybersecurity professionals to travel to foreign offices with their tools of the trade. The Proposed Rule will also remove license exceptions that allow for intra-company transfers of encryption software without an individual validated export license.

The removal of these license exceptions will create significant burdens on U.S.-based multinational companies to use the software they buy from U.S.-based companies to evaluate their security posture. This could create situations where a domestic U.S.-based security product is seen as less desirable than a foreign solution due to the need for export licenses to use the U.S. security products at foreign sites or to allow foreign national employees to use the software that originated from a U.S. vendor.

These concerns persist despite BIS’ assurances made outside the formal rule-making process that it does not intend to hinder legitimate cybersecurity activities.

I. BACKGROUND OF THE PROPOSED RULE

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (“Wassenaar”) is a multilateral export control regime with 41 participating states. It was established to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.

Wassenaar members agree to implement the arrangement's controls on items and associated technology specifically described on the Wassenaar's List of Dual Use Goods and Technologies and Munitions List ("WA-LIST") through national legislation. Members have full discretion with respect to how they implement the controls, which allows them to determine their own export license policies, and to provide explanatory notes that narrow the scope of controls consistent with Wassenaar intent behind controls.

As a result of decisions at its 2013 Plenary meeting, the Wassenaar member states have agreed to impose export control restrictions consistent with WA-LIST 4.A.5 on "Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software"; WA-List 4.D.4 on "Software" specially designed or modified for the "development" or "production" of equipment or "software" specified by 4.A; and WA-4.E.1.c on "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D." (collectively, the "pen-testing" items).

The United States principally implements its Wassenaar obligations in controls administered by the U.S. Department of State under the International Traffic in Arms Regulations ("ITAR") and by the U.S. Department of Commerce under the Export Administration Regulations ("EAR"). Accordingly, on May 20, 2015, BIS published the Proposed Rule to implement the new Wassenaar controls on exports, reexports, and transfers (in-country) of the pen-testing items.

As published in the Proposed Rule, the terms "intrusion software" and "surveillance systems and equipment" are broadly defined and would restrict exports of many commercially available pen-testing software platforms. Most of these platforms are currently controlled as encryption items, subject to the National Security ("NS"), Encryption Items ("EI") and Antiterrorism ("AT") reasons for control, and are exported in compliance with EAR license exceptions for temporary imports, exports, reexports, and transfers ("TMP") under EAR Section 740.9, and for encryption commodities, software, and technology ("ENC") under EAR Section 740.17.

Under the Proposed Rule, pen-testing items will additionally be subject to the Regional Stability ("RS") reason for control, which requires a license for export to all destinations other than Canada, and will no longer be eligible for export under license exceptions ENC and TMP or any other license exception except a select section of license exception GOV for exports to or on behalf of the U.S. Government pursuant to EAR Section 740.11(b).

The Proposed Rule indicates that BIS will favorably review license requests for exports to a United States company or subsidiary not located in Country Group D:1 or E:1, foreign commercial partners located in Country Group A:5, and government end users in FVEY partner countries (i.e., Australia, Canada, New Zealand, and the United Kingdom). BIS has also indicated that it would apply a presumption of denial to license applications of pen-testing items that have or support rootkit or zero-day exploit capabilities.

II. LIKELY IMPACT OF THE PROPOSED RULE

The proposed rule would impose a licensing requirement for exports and reexports to all destinations, except Canada, including UK, Australia and New Zealand. One intrusion software company approximates that, following implementation of the Proposed Rule, its exports of trial versions, full versions, and software updates will require 300 new license requests a year, subject to a current annual growth rate of 300 to 400 percent. A substantially larger number of new license applications will come from cybersecurity professionals that need to deploy pen-testing software to perform penetration tests and red team assessments for multinational companies and from multinational companies that need to deploy pen-testing software at their non-U.S. office locations.

A. Will Prevent Cyber Security Professionals from Doing Their Job

Cybersecurity professionals rely on pen-testing software to perform their job, and there are a variety of reasons why they must travel internationally with these tools of the trade.

Some security assessments require a cybersecurity professional to play the role of a malicious employee. During these tests, the professional may install Intrusion Software and use it to perform malicious actions until they're caught. Other assessments require a cybersecurity professional to evaluate their customer's wireless internet security, physical security, or to drop infected USB drives to see if employees pick them up and install the malicious software. These assessments help companies assess their detection and response against these attacks and each of these assessments require physical access to the company's site with the cybersecurity professional's tools of the trade available.

Other assessments require a cybersecurity professional to find vulnerabilities in a network and exploit them. The data the cybersecurity professional is able to reach with the help of Intrusion Software, after exploiting the vulnerability, will influence how quickly and fully the problem is addressed. In theory, it is possible to conduct these assessments over a VPN or from a remote Internet site. In theory, this approach is more cost effective. However, in practice, this is not how most cybersecurity professionals assess remote sites.

Cybersecurity professionals are often given a set period of time to assess a site. Two to three weeks is customary. Given that these weeks are critical, the assessment team is brought physically to the site to minimize the technical issues that could get in the way of the assessment. A cybersecurity professional's physical presence at a site is also perceived to make the assessment safer. The professional is able to exploit vulnerabilities and simulate the theft of sensitive information without that information leaving the network of the local site.

Hand carriage of a laptop and its preloaded software outside of the United States constitutes an export. Currently, EAR license exception TMP allows cybersecurity professionals to hand carry laptops containing preloaded pen-testing software to company locations outside the United States. The Proposed Rule does not allow continued use of this exception. As a result, cybersecurity professionals will need a BIS license before any travel outside the United States and Canada with their legitimate "tools of the trade."

The loss of currently available license exceptions for intra-company transfers further causes problems for multinational companies headquartered in the United States. Cybersecurity is a critical problem and multinational companies do not hesitate to hire the best talent from the countries they operate in. Security teams for multinational companies headquartered in the United States are not exclusively based in the United States. These teams often share a common pen-testing software platform to secure their United States and foreign offices.

Currently, a multinational corporation can deploy its common software platforms worldwide under EAR license exception ENC, to all of the company's offices, to improve the company's security. The Proposed Rule does not allow use of this license exception for exports of pen-testing software, which means all multinational companies must obtain BIS licenses before deployment of this very important internal asset. This could result in companies submitting, and BIS processing, a significant number of unnecessary export license applications.

B. Will Slow Development of United States Cybersecurity Technologies

Cyber attacks present a global threat that is immune to physical checkpoints. As such, collaborations with foreign partners on how to effectively generate, deliver, operate, and communicate with intrusion software is essential to the development and continued improvement of effective pen-testing software platforms. If BIS' intent is to create unnecessary obstacles to domestic participation in these international collaborations, the Proposed Rule achieves that intent.

Specifically, the Proposed Rule will restrict the ability of multinational companies to work with their own foreign offices by removing the availability of license exception ENC, which is presently used to authorize intracompany transfers necessary to the development and production of pen-testing software with encryption functionality.

C. Will Subject Most, if Not All, Export Applications to Policy of Denial

While the Proposed Rule does not seek to control exploits, it would apply a presumption of denial to license applications of intrusion software items that have or support rootkit or zero-day exploit capabilities. The problem with this licensing policy is that the Proposed Rule does not define rootkits or zero-day exploits. Both terms have different meanings depending on who is asked.

Some cybersecurity professionals define a rootkit as a technology that inserts itself below the operating system to hide post-exploitation software. Others define a rootkit as post-exploitation software that is primarily useful for maintaining control of a system without being detected after the system has been compromised.

Under the latter definition, the BIS policy of denial has the potential to prevent most pen-testing software exports. Network pen-testing software applications bundle post-exploitation software with features to maintain control of a system and avoid detection after a successful compromise. These features are necessary to help organizations test their ability to detect and respond to a successful cyber attack.

Even with a properly scoped definition, such as the former, a presumption of denial would discourage U.S. vendors from investing in technologies to emulate adversaries that use rootkit technologies. This would deny organizations a way to test their defenses against cyber attacks that use rootkits, thus making all of us more vulnerable to these technologies.

Some cybersecurity professionals define zero-day exploits as malware that attacks a software vulnerability the software's vendor does not yet know. Other professionals define zero-day exploits as malware that attacks a software vulnerability that the vendor might know, but hasn't patched.

Under the latter definition, the BIS policy of denial has the potential to prevent most pen-testing software exports, which are bundled with malware intended to test software vendor claims that their product is secure. Moreover, most pen-testing software on the market supports exploits as a necessary part of exploitation, which means the proposed policy of denial can conceivably extend to all pen-testing software depending on how BIS defines zero-day exploits.

D. Will Cause Industry Confusion

Finally, despite BIS’s ability to provide explanatory notes in the regulations, the scope of controls in the Proposed Rule are just as broad and vague as the core Wassenaar control listing. Meanwhile, BIS teleconferences and Frequently Asked Questions (“FAQ’s”) posted on the agency’s website show that the Proposed Rule does not adequately define what BIS really intends to control. As a result, the agency has thus far issued over 30 FAQs clarifying the scope of the Proposed Rule. The informal guidance does not have the force of law and many persons reading the EAR will lack notice of agency interpretations contained in the website FAQs.

III. REQUESTED REVISIONS TO PROPOSED RULE

A. Allow Greater Use of License Exceptions

1. Allow Use of License Exception TMP for Tools of the Trade

To avoid adverse impact of the Proposed Rule on the ability of cybersecurity professionals to perform vulnerability assessments and penetration tests abroad, BIS should revise the Proposed Rule to permit used of license exception TMP under EAR Section 740.9. This license exception authorizes various temporary exports, reexports, and transfers (in-country) of tools of the trade for temporary use in a lawful enterprise or undertaking of the professional.

The risk of improper use of preloaded pen-testing software exported under TMP is mitigated by the conditions for use of TMP, which require that the laptop remain under the “effective control” of the exporter or the exporter's employee and not be transferred to an unauthorized user.

In addition, BIS can implement special reporting requirements under EAR Part 743 for exports of pen-testing software under TMP. This would allow BIS and other government agencies to investigate and ensure that exports under the exception are made for legitimate end uses. To the extent that an export was made to government end users to assist in foreign intelligence services contrary to human rights or for another purpose contrary to United States foreign policy interests, BIS can seek prosecution for the unauthorized export of ITAR-controlled defense services under Arms Export Control Act or for violations of other applicable laws.

2. Allow Use of License Exception ENC for Intracompany Transfers

To avoid the adverse impact of the Proposed Rule on the ability of companies to develop new products and on internal IT professionals to use pen-testing software to secure multinational company networks, BIS should revise the Proposed Rule to permit use of license exception ENC at EAR Section 740.17 to authorize intracompany transfers of pen-testing software and related technology necessary for the development and production of company products, or for the use of pen-testing software purchased by a multi-national company for use in securing company systems and networks. Specifically, BIS should allow the use of the following:

- Section 740.17(a)(1) for exports in support of internal development or production of new products to private sector end-users headquartered in a Supplement No. 3 country for internal development or production of new products by those end-users.
- Section 740.17(a)(2) for exports and reexports to United States Subsidiaries and by a United States company and its subsidiaries to foreign nationals who are employees, contractors or interns of a United States company or its subsidiaries if the items are for internal company use, including the development or production of new products.

The risk of improper use of the software exported under these ENC sections is mitigated by the scope of EAR Section 740.17(a), which limits use of the exception to intracompany transfers and, as noted to paragraphs 740.17(a)(1)(iii) and (a)(2), all items produced or developed with items exported or reexported under ENC Sections (a)(1) and (a)(2) are subject to the EAR. In addition, same as noted in the case of license exception TMP above, BIS can implement special reporting requirements for exports of pen-testing software under ENC to provide the government with visibility into use of the exception.

3. Allow Use of License Exception TSU for Operation Technology and Software Updates

To avoid the adverse impact of the Proposed Rule on the ability of companies to support customers by providing answers to basic technical questions on software use and operation, train customers on use of the software, and provide other necessary operation technology; and to provide software updates in support of customer use of lawfully exported products, BIS should revise the Proposed Rule to permit use of the license exception for technology and software – unrestricted (“TSU”) at EAR Sections 740.13(a) and (c).

The risk of improper use of the software exported under these TSU sections is mitigated by the scope of EAR Section 740.13, which limits use of the exception to operation, maintenance and repair technology; to operation software, in object code, that is the minimum necessary to operate equipment authorized for export or reexport; and to updates that are intended for and are limited to correction of errors (“fixes” to “bugs”) in software lawfully exported or reexported (original software). Further, under the exception, such software updates may only be exported or reexported to the same consignee to whom the original software was exported or reexported, and such software updates may not enhance the functional capacities of the original software.

In addition, as noted above in the case of license exceptions TMP and ENC, BIS can implement special reporting requirements for exports under TSU to provide the government with visibility into use of the exception.

B. Include a Definition for Zero-Day Exploits

As noted above, the Proposed Rule fails to define what constitutes a “zero day exploit,” the presence of which in a pen-testing software platform would subject an application for export of the software to a presumption of denial. To properly define the scope of its presumption of denial for exports of pen-testing software, BIS should adopt the following definition:

Zero-Day Exploit: A software tool that takes advantage of a security vulnerability that is not publicly known. Security vulnerabilities will be deemed publicly known if: (1) they are the subject of a published notice or advisory that is generally available to the public; or (2) Forty-five (45) days have passed since the vulnerability was reported to a software developer or a vulnerability reporting organization.

C. Do Not Implement a Presumption of Denial for Rootkits

The Proposed Rule also seeks to apply a presumption of denial to exports of pen-testing software packages that include a “rootkit.” However, as noted above, a rootkit is another method to avoid detection and it falls within the scope of Intrusion Software generally. Because of this, BIS should not subject applications for the export of pen-testing software to a presumption of denial merely because the software package contains a rootkit.

D. Integrate FAQs into Explanatory Notes Within the Regulations

To clarify the correct scope of the new Wassenaar controls, BIS should accurately reflect what the agency intends to control by inserting substantive parts of its website FAQs into the explanatory notes of relevant EAR Part 772 definitions and/or Part 774 Commerce Control List entries.

E. Issue Another Round of Proposed Rules

This is a complicated issue and it is important that the final rule does not hamper legitimate cybersecurity practices. BIS should therefore issue another proposed rule and provide another period of public comment.

Thank you for your consideration.

Yours truly,

ON BEHALF OF THE FIRM



Matthew A. Goldstein, Principal Counsel

MATTHEW A. GOLDSTEIN, PLLC

1012 14th Street NW, Suite 620

Washington, D.C. 20005

Tele: (202) 550-0040

Email: matthew@goldsteinpllc.com

PUBLIC SUBMISSION

As of: July 27, 2015 Received: July 19, 2015 Status: Posted Posted: July 27, 2015 Tracking No. 1jz-8k2k-tyig Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0109

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nicholas Kain

General Comment

I develop secure software systems, often related to low-level networking, and in order to do that, I keep up with and sometimes research software vulnerabilities.

""equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially""

This segment of text seems to be written by someone who has a false understanding of how computing systems work. It will either ban every development tool or no development tools, because unlike most professions, our tools are constructed by our tools without limit; the best analogy is to that of carpenters or metalworkers, who make their own jigs, but we have no limits -- we craft our own saws, tables, measuring equipment, everything. Therefore 'specially designed for the generation of ... software' is either overly broad (a ban on all development tools, such as debuggers, compilers, assemblers, or at a lower level, tools of hardware engineering such as logic analyzers, oscilloscopes, IO-interfaceable FPGAs...) or simply nonsense.

""designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology

required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components thereof, and development""

The same flaws apply to the reasoning around 'IP network ... production equipment'. This would seem to be a ban on all internet-compatible networking systems. IP is generic -- it functions much like postcards put in the postal service mail, with a destination address. Producing these packets is easy and part of the normal functioning of virtually all modern networking systems.

I can be somewhat sympathetic to the intention to restrict the export of systems of mass surveillance. However, the wording in this document is overly broad and would do far more than that -- it would effectively restrict the production of ANY networking software or hardware, regardless of purpose.

Restricting systems of mass-surveillance would be better done by language that attempted to restrict the export of systems designed to function at a certain scale (eg, a certain number of packets recorded per second) or implementation of restricted capability commercial off-the-shelf products (eg, black box devices that when attached to the network would record all traffic, such as an integral fiber-tap + recording hardware system).

""and production software and technology thereof. BIS proposes a license requirement for the export, reexport, or transfer (in-country) of these cybersecurity items to all destinations, except Canada. This rule also sets forth proposed license review policies and special submission requirements, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items and information security functionality.""

The proposed limitations would severely damage the ability for American engineers and researchers to perform their jobs, and would damage the competitiveness of American businesses that rely on the productivity of these engineers and researchers. The likely outcome would be for many engineers and researchers to relocate to other countries where they could perform their jobs. Businesses would likely either do the same, or hire foreign workers to perform jobs formerly performed by domestic workers. This effect can easily be seen by looking back to the era of export restrictions on cryptography, where businesses and individuals located in America were at a severe disadvantage because of the onerous requirements that foreign entities were not subject to.

Please do not make the mistake of implementing these rules as they stand -- they are more restrictive and would be a greater burden to us than ITAR was for cryptography in the 90s.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2p-8088
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0110

Comment on FR Doc # 2015-11642

Submitter Information

Name: Kevin O'Connor

General Comment

This will just lead to job losses, movement of development outside of the country and divert skilled researchers to other countries; some not as friendly to our policies.

Design and production will continue regardless of policy.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2p-kf66
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0111

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

I am a cybersecurity professional working for a large U.S. technology company. It is my job to ensure the security of my company's network and information assets, using a wide array of detective, preventative, and investigative tools.

In response to question 3, "Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks?":

1. Many of the tools that I use would be classified as intrusion or surveillance items under this new rule. For tools purchased from a commercial vendor, the vendor would have the financial resources necessary to comply with this new licensing process. However, a substantial number of these tools are developed via the goodwill of open-source communities, where no such resources exist. The effect of this rule on these open-source communities would be devastating, and cause the development of these tools to cease for fear of prosecution. The lack of availability of these open-source tools and the open innovation that they engender would have a direct negative effect on the security of my company's network, and the networks of all other U.S. companies.

There needs to be language added to this rule that protects the free distribution and use of open-source cybersecurity tools for research, auditing, testing, and other purposes that promote protection from cyberattacks. By their very nature, such open-source tools are distributed in

ways that do not advantage any one party more than any other, and promote learning and understanding of cybersecurity issues rather than their exploitation for private gain. If the goal of this rule is to prevent the private sale and export of cyber "weapons" to parties that would use them for nefarious purposes, then it should be possible to add language protecting these open-source tools without diminishing the rule's primary intent.

2. On at least one occasion I have found a zero-day vulnerability in a piece of software, and reported the vulnerability to the software vendor so that they could fix it. In that process, for practical reasons I was required to develop "proof-of-concept" code that demonstrated exploitation of the vulnerability. There does not appear to be any language in this new rule that protects this kind of responsible vulnerability disclosure. In fact, under the paragraph entitled "License Review Policy for Cybersecurity Items", there appears to be language that may significantly impede it:

"Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities."

There needs to be language added to this rule that specifically protects the responsible disclosure of vulnerabilities, which may include the transmission of proof-of-concept exploit code across state or international boundaries. This protection is absolutely necessary for cybersecurity professionals like myself to be able to report vulnerabilities without the encumbrance of obtaining export licenses or fear of prosecution from not having done so.

To put it in perspective: if I had been discouraged by a rule such as this from reporting the vulnerability that I found, then the vulnerability would still be present in computer systems used today by millions of U.S. citizens, and would still be exploitable to the detriment of those citizens by anyone else who might have also found it.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2p-n96x
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0112

Comment on FR Doc # 2015-11642

Submitter Information

Name: Ozan Munsuz

General Comment

This will do NOTHING and i repeat NOTHING to stop the blackhats. What it will do however is make it a pain to obtain some of the tools to test our own networks to keep them from the blackhats. Remember the encryption restriction. We all saw how well that went. It was rolled back due to it's stupidity even if this does pass the same thing will happen to this.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 19, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2q-67tf
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0113

Comment on FR Doc # 2015-11642

Submitter Information

Name: Andrew Pietila

Address: United States,

Email: me@ajp.xyz

General Comment

Wassenaar's spiele on Intrusion and Surveillance Items is an unwarranted intrusion on people who author software legitimately.

Consider the following. In Chicago, they are well known for having overly strict gun laws. Most of which if challenged by a decent lawyer would probably be deemed unconstitutional. And yet there are 7 causalities per day, mostly wounding although it's not uncommon for a kill, caused by projectile-based weapons. Many people who perpetuate these crimes don't have a right under Chicago and related jurisdictions to carry a weapon.

Lets turn back to the proposed terms on Wassenaar. This time, lets go to Italy, and the recent Hacking Team incident. Horrible name for a crew, but that's besides the point. They proclaimed publicly to be Wassenaar-compliant. They claimed it previously, they claimed they've always been compliant with the law. And yet, it takes someone illegally breaking into their systems to find out, oh, they aren't so compliant. They've been selling software to countries that they don't have a right to sell software to. They've been developing exploits that here in America if utilized would carry a penalty that would scare a man like Aaron Schwarz to suicide.

But not only is the proposed terms on Wassenaar unenforceable, there's a strong likelihood that it's unconstitutional.

Consider *Bernstein v USDOJ*, 922 F. Supp. 1426 (N.D. Cal. 1996). The court found that the prohibition of exporting encryption software was a violation of the First Amendment's provision disallowing laws enacted to abridge the freedom of speech. This was upheld in the 9th circuit court of appeals. What we are proposing is the forbidding of a different class of software, one designed to do a different task. Yet, it is my belief that this software too is protected by the same freedom of speech as software that provides encryption stronger than 40 bits of strength.

So to sum things up, Wassenaar's provisions on Intrusion and Surveillance items is an unenforceable mess as well as an abridgement on freedom of speech, and is as such likely unconstitutional. That is why the proposed docket item must not be enacted.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2t-bo7a
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0114

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nate Lawson

Address:

4096 Piedmont Ave
Suite 138
Oakland, CA, 94611

Email: nate@root.org

Organization: Root Labs

General Comment

Dear BIS,

I'm writing to oppose the regulation of a class of software loosely called "intrusion software" in this agreement. To do so would be directly in conflict with the First Amendment right to free expression and also severely hamper the research we rely on to secure the Internet today.

I have worked in computer security and cryptography for 20 years. If you review the history of the cryptographic export restrictions of the late 1990's (ITAR), you can see the parallels. The export restrictions, which regulated cryptography in a manner similar to munitions, led to US-based businesses being vulnerable to numerous compromises due to poor crypto designs and insufficient key length to comply with them.

Even today in 2015, major security flaws are compromising encrypted communications as a direct outcome from the export restrictions which ended at the turn of the century. The SSL protocol has had several critical flaws recently due to a fallback mode that was included to

support the so-called "export ciphers", and that mode wouldn't have existed without the misplaced ITAR restrictions back then.

Please do not attempt to turn back the clock on security research, attempting to regulate the free speech required to perform open exchange of information. Such attempts will only hamper legitimate research, make US-based businesses less competitive, and stifle an area where we should be leading. The security of our own businesses depends on security (and crypto) research continuing to make rapid developments that unnecessary regulation will hurt our country immensely.

Please decline to regulate security tools as the unintended consequences are too great.

Sincerely,
Nate Lawson

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2u-mhf5
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0115

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matthew Murphy

Address:

352 Brighton Ave

Apt 327

San Francisco, CA, 94112

Email: matthew.r.murphy@me.com

Phone: 14084764265

Organization: Uber Technologies, Inc.

General Comment

I work as a security engineer for a technology company. My work is entirely defensive in nature: my sole charter is to protect the company, its customers, its partners and their respective data, from threat. Yet, the proposed rule would tremendously impair my ability to do my job, as I would face considerable regulatory ambiguity and risk.

The proposed rule's definition of "intrusion software" covers the vast majority of the tools I have built or might build to protect my employer's infrastructure. For example, if I write an attack tool in an attempt to find components of my employer's infrastructure that suffer a particular security issue, that tool is intrusion software under the proposed rule. I would, under the proposed rule. In order to defend our infrastructure, I must be able to utilize substantially similar techniques to those who would do it harm.

My employer utilizes a number of third-party companies as service providers, and many of these companies are located outside the United States. It is not difficult to imagine a

circumstance where I review the systems of a third-party partner, find a security issue, and am unable to provide any means to reproduce and address that issue because the tooling that would replicate it is a regulated export under the proposed rule. The rule would vastly weaken arms-length and/or open-source collaboration between enterprises and people with similar security interests. That is vastly more damaging to people seeking to protect themselves than it is to potential criminal or nation-state attackers.

On balance, the proposed rule makes legitimate knowledge sharing even more difficult than the maliciously-intentioned exports it seeks to prohibit. Those who are willing to sell their tools to nation-states or other ill-intentioned actors likely will not be bothered by doing so at regulatory peril. I, on the other hand, certainly will, as my career and livelihood would be irreversibly harmed. It is likely that the proposed rule would make the Internet security situation worse, by chilling the speech of the very people who work tirelessly for its defense.

I would advise that BIS redraft the rule, with more focus on the intent of the exporter and/or the post-compromise stage of the intrusion software tool chain. That is, limit the prohibition of intrusion software to those who, with intent or by gross negligence, distribute a tool to a party with malicious intent; or focus the rule on software that seeks to surveil compromised systems and report back to an initial intruding actor. Even a narrower rule could have serious unintended consequences, so BIS should subject any redraft to an additional comment period.

The potential adverse impact of a bad rule is so severe that it's far more important to do the rule-writing narrowly and precisely than to do it quickly. In general, BIS should err toward specific, narrow regulations that perhaps miss some categories of actor, than toward over-broad regulations that harm essential research. It is important for BIS' rules to be implementable with industry support, or they are likely to make matters worse, rather than better.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2x-rv32
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0116

Comment on FR Doc # 2015-11642

Submitter Information

Name: James Ford

General Comment

I oppose the proposed rule. Security depends on transparency. Restricting the flow of information will only lead to more problems down the road. Numerous security researchers have already echoed this comment below so I am only posting to provide my support and agreement with their conclusions.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k2x-orrc
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0117

Comment on FR Doc # 2015-11642

Submitter Information

Name: Craig Nelson

General Comment

I oppose this. Regulations and barriers to distribution of such software will just reduce transparency on the security of software and overall result in more security issues, since it will inhibit testing and knowledge sharing.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k32-y8bu
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0118

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

See attached

Attachments

WA Comments

Comments on the Wassenaar Arrangement proposal by the Bureau of Industry & Security
From a US citizen living abroad interested in Information Security and wanting to get into the field

20th July 2015

Following the news on the BIS proposal for implementing the Wassenaar Arrangement in the United States, it troubles me to learn that the field that I wish to get into is coming under attack by overly broad and vague rules, with restrictions mainly intended for military applications as evidenced by the broad categories defined in the list of restricted technologies¹

Although I am not an information security professional, it is the field that has most interested me in my work with computers and something I strongly want to pursue and have been in my own spare time. These overly broad rules, that even information security professionals cannot interpret², send a chilling effect to those who wish to venture into the field, as well as those who are already in it. It takes away the life and livelihood of many people who are interested in the security of the Internet, while hampering their ability to do their jobs effectively.

These regulations will not stop some research, nor will they stop the vulnerabilities from existing, from being found and from being exploited. Research into things has never been stopped by regulation and law; it is merely driven underground. The net effect of the BIS proposal as seen will have those that they wish to impede still researching and developing and those who are trying to defend unable to or wary of the consequences of trying to find the same vulnerabilities and disclose them in a responsible manner.

As a US citizen living in a foreign country, whose authority do I have to bend to? Should I myself find a vulnerability, the act of transmitting it to my government as proposed by the BIS could run afoul of my host country, which also happens to be a member of the WA. Regardless of that, this should never happen. As a US citizen, I mistrust my own government and what they would do should something like this come to pass. It must never be allowed to require you share vulnerabilities with your own government.

With the recent exposure of Hacking Team, the US government has paid for the very thing that this proposal is trying to control³. This incident some would regard as a poster child for needing these strict regulations, actually shows the opposite; it shows that we need open research and open collaboration to defend better against these situations, as well as making a livelihood. As has been shown, the WA did absolutely nothing against HT, as they had a global license⁴ and these regulations are ineffective at doing what is proposed⁵.

Trying to regulate knowledge is not democratic; some would argue, in my estimation rightly, that code is akin to speech. Trying to regulate the transfer of knowledge itself is wrong under any form of democratic government. Knowledge is inherently neither good nor evil; it is the application of that knowledge judged by morals that makes it so. Should these proposed regulation occur, it only hampers the defense of the internet; it will not stop those who it is intended to stop.

This proposal deeply concerns me, not only as someone wanting to get into the field of information security, but as a human. Trying to restrict the flow of knowledge between people for what can be conceivably be considered as no gain is downright deleterious to society as a whole, creating more vulnerability in an already vulnerable world, and setting a dangerous precedent for the gaining and sharing of knowledge. No, I do not have any specific proposals, as I have not breached the field yet; however, I would suggest listening to those who have submitted proposals, particularly those by

¹ <http://www.wassenaar.org/controllists/2014/WA-LIST%20%2814%29%202/WA-LIST%20%2814%29%202.pdf>

² <https://lists.alchemistowl.org/pipermail/regs/2015-June/000294.html>

³ <https://wikileaks.org/hackingteam/emails/emailid/1108899>

⁴ <https://twitter.com/thegrugq/status/619524311011885056>

⁵ <https://twitter.com/thegrugq/status/619343359501447169>

respected security companies, security researchers, and others in the field who have more experience than I do.

Yours,

A concerned US citizen living abroad

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k32-j51e
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0119

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

What is being proposed is too broad and vague in its scope and application as worded. As proposed it looks like it would only hamper the people and/or entities, who try to abide by the laws/regulations and, do nothing to solve the actual issue.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k33-f9om
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0120

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nicholas Weaver

Address:

1947 Center Street suite 600

Berkeley, CA, 94704

Email: nweaver@icsi.berkeley.edu

Phone: 510-666-2903

General Comment

There is an essential need for a second round of comments after any changes are made in response to this feedback process.

It is clear that the security community has significant problems with some of the details (such as the lack of a blanket exemption for intra-company transfers), and has offered multiple suggestions which can help maintain the spirit of the Wassenaar rules while mitigating much of the collateral damage.

As just one minor example of a perhaps unintended result: Wassenaar rules, as written, may cover counter-censorship systems:

Counter-censorship systems extract information from the network, and are specifically engineered to evade Network Intrusion Detection Systems, as censorship systems are fundamentally equivalent. (As an example of how counter-censorship is NIDS evasion, see Khattek et al, "Towards Illuminating a Censorship Monitor's Model to Facilitate Evasion", FOCI 2013, <http://www.icir.org/vern/papers/censorship-model.foci13.pdf>). And although it is

clear the intent of the proposed regulation is to prevent exfiltration of data, the actual text:

"(a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data"

does not have a notion of consent, so although a counter-censorship system takes information from the network and returns it to the client, it might still be classed under "extraction of data or information" from the remote systems.

A minor change, "without the user's consent" would eliminate this ambiguity, as it is clear that there is no intent to place censorship-evasion tools under Wassenaar.

There are numerous other such comments (this author has also provided a suggested exception for Network Intrusion Detection Systems under the definition of "Internet Surveillance").

With the large number and detailed technical nature of the comments, it is essential that these proposed rules are created in a two part process, where this initial round of public feedback results in a set of modifications, with another round of public feedback to ensure that those modifications are sufficient to mitigate the critical concerns of those responsible for securing our computer systems from attack.

-Dr Nicholas Weaver, Ph. D.
Researcher, International Computer Science Institute
Title for identification purposes only.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k33-qute
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0121

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

I am a security researcher with 15 years experience. These rules seem overly broad in a way which would severely impact the good guys. The ability to test systems and pick apart security vulnerabilities and tools and share findings with other good guys is crucial to the security of the internet and computing world wide.

The result of broad rules crafted without a full understanding of the issues and landscape is likely to create unforeseen consequences which cause harm and set us back in our collective mission to make the internet a safer place for all.

Please reconsider these provisions.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k33-rsp3
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0122

Comment on FR Doc # 2015-11642

Submitter Information

Name: Paul Nash

Address:

100 Minot Road

Concord, MA, 01742

Email: pnash@mac.com

General Comment

Hello,

I've worked in the Information Security field for approximately 20 years. As part of a Boston security think tank, LOpht Heavy Industries, I was interviewed by numerous magazines, newspapers & websites - most recently in the Washington Post, regarding internet insecurities. I was a founding member of a premier information security consulting firm and have consulted for Fortune 100 organizations, worked with individuals in the White House, as well as conducting security related research that has been used to detect and identify threats and attacks against what has become critical infrastructure. In order to properly secure organizations and minimize risk, I've identified vulnerabilities in software and have worked with vendors to mitigate my findings.

I'm concerned about the potentially unforeseen impact or unintended consequences of these new cyber regulations will have on the information security community, security research, and the information security industry.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k33-97i5
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0123

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jonathan Walker

General Comment

Comment on FR Doc # 2015-11642

The proposed Wassenaar Arrangement (WA) is hazardous to not only companies who intend to protect the public and private companies, but also to security research globally. This may hinder vulnerability research, screening a company's ability to protect clients, and also audits that occur internally within an organization. Although I appreciate its intent to prevent exploits from being sold commercially and allow for intrusion software to be sold in oppressive regimes, this is certainly not the way to do so.

This will certainly hinder the cyber security industry and make us all more open to attacks. I also appreciate allowing for non-proprietary research to allow for security vulnerabilities to be reported responsibly to the effected individuals. Although this may also prevent organizations from offering incentives by responsibly reporting vulnerabilities that a large amount of leading industry leaders offer. Although the underlying issue needs to be addressed, the wording is far to broad and encompasses individuals without malicious intent, with the intention of protecting the general public from cyber security threats.

Sources:

<https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation>

<https://community.rapid7.com/community/infosec/blog/2015/06/12/wassenaar-arrangement--frequently-asked-questions>

<https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>

<http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>

Jonathan Walker
Bachelors in Network and Security
Cyber Security Researcher and Instructor
Linux Systems Administrator

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k33-lu5i
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0124

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jonathan Janego

Address: United States,

Email: jonjanego@gmail.com

Phone: 312-561-3115

General Comment

I'm a security engineer at an application security company based in Massachusetts, and I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k34-tfnd
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0125

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael VanZant

General Comment

If you do this, you are crazy. Don't do this!!! Besides, computer code is speech.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k34-217p
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0126

Comment on FR Doc # 2015-11642

Submitter Information

Name: John Doe

General Comment

See attached file(s)

Attachments

letter-bis-out

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B, U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security

To the Bureau of Industry and Security, regarding BIS-2015-0011

I write this letter to you after carefully considering not to, given the deplorable state of affairs involving the public discussion of the Wassenaar Arrangement (WA), in places like Twitter and other (online and otherwise) venues. I do not consider the opinions of either sides (those in agreement and those opposing the WA) to be completely honest. Since my time is limited, I will try to convey what I believe is a truthful account of the situation, as it affects the security community and those involved in activities affected by the WA, in as few words as possible.

First I will enumerate the major points of concern, from the perspective of someone who understands both the offensive and defensive needs of the industry, the government, and the general public, and how these apparently opposed sides of the same coin seem to be conflicted with one another.

To the best of my knowledge:

1. In the past five years, the market for unpatched, previously unknown vulnerabilities, otherwise oft referred to as "zerodays", has bloomed far beyond the limited, tightly knit close circle of researchers and buyers (big game defense contractors the likes of Mantech, Harris and Raytheon). The only common denominator thus far is the lack of transparency and irregular (not necessarily illicit, but almost always of questionable business ethics) dealings, where the researchers are in an immutable position of vulnerability, with no access to information such as final sales figures, itemized contracts (even if sanitized) or the exact amount taken from such sales by the chain of middlemen between the researcher and the final customer, often a federal government agency.
2. Several companies have been reviled publicly for engaging in these deals, both domestic and foreign. While major defense contractors such as Raytheon, Mantech, Terremark or Harris might be involved, and suffer of the same lack of transparency or abusive business relationships with researchers, it is middlemen like Vulnerabilities Brokerage International,

Netragard and a myriad of other, *very private small businesses*, based on Massachusetts, Michigan, Florida, California, New York and other states, *many of these unheard of*, incorporated as LLCs with little to no public history, and often employing foreign nationals, often off the books, that are actually producing and selling the bulk of offensive security research used to compromise foreign and domestic individuals and businesses, as well as government networks.

3. Through leaks such as the most recent Hacking Team incident, the public has only managed to catch a glimpse of such deals. However, most of the activity, which happens within US borders and involves US businesses, has not surfaced, nor the identities of those involved have been sufficiently established and exposed.
4. In some cases, consulting companies offering security services to major software corporations, such as IOActive recently, have been exposed as being actively involved in the trade of zeroday exploits, in what could constitute a significant conflict of interest.
5. The actual funding, whether it comes through existing contract vehicles, or service contracts offered and managed by major defense contractors, is still US tax payer money, subject to stringent rules of transparency that are apparently not applicable for a selected few.
6. It must be noted these are private businesses and not the federal government, without any kind of oversight, disposing of federal government money.

Because of these circumstances:

1. The WA is apparently of no relevance to the aforementioned trade or business deals, only impacting the security community negatively, while leaving these private businesses free to operate in the legal vacuum they have enjoyed since their inception.
2. While the above statement is true, it is also true that many security professionals, who did not hesitate to "turn coats" from a pro-disclosure (of security vulnerabilities) stance to a non-disclosure stance (for the sole purpose of profiting from zeroday sales) are crying wolf about the WA, as if it affected their publication and sharing of vulnerabilities or security work, when in reality, they have no intention to do so, and currently most of what is published is the tip of the iceberg compared to the flux of information and tools to exploit unknown vulnerabilities, that are being sold, marketed and procured to the federal government and foreign parties (as demonstrated in leaks such as that of the Hacking Team files, which prove the sale of zeroday exploits by a small-game US middle-man company, Netragard, to a foreign entity).
3. Until the WA actually becomes an incentive for transparency and fairness towards the most vulnerable element of both the market for vulnerabil-

ities and the security community (the researcher), and actively punishes or draws the line for middle-men and private companies catering to the federal government, its usefulness will only amount up to a feeble attempt at window dressing, while America keeps on outsourcing its most intimate and delicate matters to private businesses enjoying non-existent oversight and accountability.

While I do not believe the recent incidents of exposed businesses involved in this trade (mostly foreign, suspiciously enough) are something to celebrate, and they distract and remove attention from the places where it might be most needed, they do serve as an example that the security industry, after years of feeding off hype and contradicting its own claims of morality and ethics, should take a moment to introspect and wonder if the WA, or future attempts at regulation of these practices, however they turn out to be, are not the natural consequence to infantile dwellings and assorted nonsense, as observed in Twitter and elsewhere. You can only wait so long after you make the bed, to sleep in it.

Yours truly

John Doe and sobergrugq

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-v9i1
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0127

Comment on FR Doc # 2015-11642

Submitter Information

Name: Peter Hesse

Address:

13454 Sunrise Valley Dr.

Suite 440

Herndon, VA, 20171

Email: peter.hesse@10pearls.com

Phone: 703-935-1951

General Comment

The attached document "Peter Hesse RIN 0694-AG49 Comment.rtf" contains my comments upon the proposed rule regarding Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, also referred to as RIN 0694-AG49. My comments run longer than the allowed size of the web form for submission.

Peter Hesse

Chief Security Officer

10Pearls, LLC

Attachments

Peter Hesse RIN 0694-AG49 Comment

The following is a comment upon the proposed rule regarding “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items”, also referred to as RIN 0694-AG49.

I am an individual who has been involved in both government and private sector information security since 1995. My experience covers a wide area including security controls (such as anti-virus, firewalls, and intrusion detection/prevention), cryptography, public key infrastructure, and security assessment of both organizations and systems. I am very concerned about the potential wide-reaching impacts of this proposed rule as it is currently written. I have two main concerns that form the basis of my comment. First, that offensive or attack tools have a use in defense. Second, that the rule will eliminate responsible vulnerability disclosure. Both of these concerns have the same end state: that our information security will actually be reduced by this proposed rule.

—== Point 1 — The rule cannot differentiate between tools used for offense or defense ==—

One of the things that sticks out most in my mind was the presentation I saw provided by Pieter (“Mudge”) Zaitko, very soon after he was tapped to lead the Defense Advanced Research Projects Agency (DARPA) Cyber Fast Track (CFT) program. His talk captured the attention of many attendees, both public and private sector. The audience was filled with some who would be considered “hackers”, who sought to legitimize hard work already accomplished, as well as find ways to fund new ideas in the area of cyber security. I remember him telling the attendees that the CFT will be able to fund any work that has a defensive component or concept to it. This meant that CFT would not be used for funding “offensive weapons” that made hacking easier, but instead “defensive protections” that made hacking more difficult.

The very next statement he provided is the most important thing for the Government to understand regarding this proposed rule: “If you think your idea is only able to be used in an offensive capacity, you haven’t thought your idea through well enough.” Zaitko understood, as did

many of the more experienced information security individuals in attendance, that all offensive capabilities can also be defensive capabilities. Probing your own defenses is an extremely important form of defense in this day and age of advanced cyber security concerns.

The current plan for this proposed rule does not allow for a notion of an offensive, intrusion, or surveillance tool to be used in a defensive or preparatory capacity. Indeed, it would be nearly impossible to differentiate when the same tool is used in these varying ways. This rule could have a chilling effect when it comes to our own network defenses, which is exactly the opposite of the intention.

Until this proposed rule can be written in such a way that it can allow for “offensive” tools to be used for “defensive” purposes, and without this being a judgement call provided by an expert (or worse, a bureaucrat that doesn’t understand the technology), I would strongly recommend that the proposed rule is not accepted.

—== Point 2 — It will eliminate responsible vulnerability disclosure ==—

The BIS FAQ basically directly describes the fact in item 4 that vulnerability disclosure would be considered controlled under the proposed rule. The consequences of eliminating vulnerability disclosure are very direct. Responsible vulnerability disclosure is defined different ways by different individuals; the concept is to inform a manufacturer of a vulnerability, allow the manufacturer to fix it, and then disclose the vulnerability publicly to inform the community at large. Some feel that only a certain time should be given between informing the manufacturer before going public, others believe the manufacturer should always be allowed to complete the fix before going public.

Responsible vulnerability disclosure has two indisputable powerful effects on security in our era. First, it has forced manufacturers to improve security and improve their ability to patch because of the threat of potential public disclosure. The tremendous improvement of

security at software providers such as Microsoft, for example, demonstrates how effective this has become. The second, is that public disclosure allows a sharing of thought processes, such that others can build upon one exploitation method to develop another. For example, after the first vulnerability to use a buffer overflow as a mechanism to break software was disclosed, other vulnerabilities were quickly developed to use the same mechanism on other products and systems. This sharing in the creative thought process would be eliminated, causing again a net negative effect on security.

Until this proposed rule can specifically permit responsible vulnerability disclosure, I would strongly recommend that the proposed rule is not accepted.

=== Conclusion: The Proposed Rule reduces security ===

By disallowing the use of offensive or attack tools to improve defenses, our defenses will get weaker, and yet still be exploited by criminals that do not follow the law. By disallowing responsible vulnerability disclosure, the industry will have little reason to push further and faster with security improvements, and the creative thought process around defensive protections will be stifled. The end result of the current proposed rule would be a reduction in information security across the board for all those affected by the legislation.

=== Responses to BIS request for comments items ===

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:
 - a. How many additional applications would be for products that are currently eligible for license exceptions?
 - b. How many additional applications would be for products that currently are classified EAR99?

>> This would not directly impact our organization at this time, but it would impact organizations from whom we acquire services and

applications.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

>> As we understand the rule, we would need to on the order of a dozen applications a year, where we currently do not submit any.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

>> Please see responses above regarding the first point, about differentiating between tools used for offense or defense.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

>> It would take approximately 1 week per application, so up to 12 weeks per year of effort. It is not information already in place for products.

Final Recommendation

I would also like to formally recommend at least one more round of draft regulation and comments. I do not believe this proposed rule has had enough time to be properly considered, or the potential consequences of this action to be understood.

Sincerely,

/pmh/

Peter Hesse

Chief Security Officer

10Pearls, LLC

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-ircv
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0128

Comment on FR Doc # 2015-11642

Submitter Information

Name: Russel Van Tuyl

Address: United States,

Email: Russel.VanTuyl@gmail.com

General Comment

I'm a penetration tester working for an enterprise information security firm. I'm concerned how with how this regulation is going to effect the community, the security industry, and U.S. businesses at large. Unforeseen impacts my impair my ability to provide valuable service to organizations looking to increase their cyber security posture. Regulations should enable security practitioners to raise the bar on information security, provide services that will enhance the nations ability to defend itself from cyber attacks, and to lead the world in research & development. I'm also concerned about having tools, techniques, and procedures removed or regulated in such a fashion that will negatively impact the information security industry and its ability to defend and protect against adversaries.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-olly
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0129

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

See attached file.

Attachments

Cybersecurity Comment

Introduction:

As a global auto manufacturer we are pleased to provide comments to the U.S. Department of Commerce, Bureau of Industry and Security on the Export Administration Regulations (EAR) proposed rule (Department of Commerce Bureau of Industry and Security, 80 Fed. Reg. 28853) proposed, May

20, 2015, hereinafter “Proposed Rules.” We understand the proposed rules in question are in furtherance of BIS’ duty to implement the agreements of the Wassenaar Arrangement at the December 2013 Plenary meeting. While we appreciate the difficult undertaking that accompanies this effort, we believe the proposed rules add regulatory complexity, licensing uncertainty, and will have immediate impacts impeding vehicle and IT network cybersecurity.

Our company faces numerous cybersecurity threats daily and our ability to perform penetration testing and cybersecurity research is vitally important to our customer’s safety and the operation of our business. If BIS adopts the proposed rules, many items previously classified EAR99 will become export controlled and subject to onerous and extensive licensing requirements and restrictions.

Deemed Export Analysis:

Our company performs cybersecurity threat research and penetration testing on our vehicles and network infrastructure to ensure customer safety and the integrity of our networks. Many of the tools currently used are classified EAR99. If the BIS proposed rules are implemented our deemed export license requirements will go up dramatically. Furthermore, the impact to BIS for licensing will not be inconsequential.

Our company, like many others, hires foreign national employees and contractors for a variety of positions, including those relating to cybersecurity. The information technology industry overall has a large foreign national presence and our IT department is no different. While our company requests deemed export licenses when necessary, the proposed rules will necessitate a dramatic increase in the number of BIS licenses requested. Further complicating the licensing process will be BIS’ case-by-case license review process. A case-by-case review of every license request will add uncertainty to a process that should be very straightforward. These processes add both needless time and uncertainty to companies that are under constant threat of cyber-attack.

In addition to the case-by-case licensing review stated above, the proposed rules include “Supplement No. 2 to Part 748-Unique Application and Submission Requirements for Cybersecurity Items.” Supplement 2 to Part 748 adds licensing requirements for cybersecurity items requiring the applicant to answer a series of highly detailed questions as part of each license application. Providing the Part 748 answers will require the exporter to do a lot of product research and investigations on products, most of which are provided by third parties. We will have to send our questions to the item manufacturers and await their answers, in order to complete the licensing package while we may be under a network attack.

The proposed rules also remove all license exceptions except GOV. License exceptions provide an invaluable service for exporters that have very routine exports such as internal cybersecurity research and penetration testing items and technology. The elimination of license exceptions ensures we will have to go to BIS for a license, which will create a slowdown in our internal processes. Licensing for formerly EAR99 items, Supplement No. 2 question requirements, and removal of license exceptions creates an intolerable slowdown in our ability to provide for customer safety and network integrity.

Export Analysis:

In order to protect our customers and networks we need to share cybersecurity items and technology in and among all of our global locations. Cybersecurity threats can and do occur globally and can originate in one country and spread to others. In order to guard against such an attack, cybersecurity research and penetration testing often times begin in the U.S. and extend to non-U.S. locations. In order to perform this work we will have to export cybersecurity items and technologies, which will now require BIS licenses for many items currently EAR99. As with deemed export licensing, BIS will review licenses on a case-by-case basis. This type of review will most certainly slow down our ability to secure our vehicles and networks. Additionally, we will be required to provide answers to the Supplement No. 2 Part 748 questions in all license applications. With the removal of all license exceptions except GOV our ability to provide for customer safety and network integrity will be greatly compromised.

For example, if we encounter a global threat or intend to do a new project to validate our network infrastructure in the U.S., we will need to apply for deemed export licenses so that our foreign national employees may participate. In order to thoroughly continue the project we would then need to share items and/or technology with other corporate locations globally, which will require export licenses of both the tools, but also any associated technology. Once those items are at their foreign destinations, deemed re-export, and item re-export licenses may be required in order to transfer those items to other company locations. Because the licensing process can take 30 days or more and with the imposition of additional requirements, cybersecurity projects will be jeopardized. The cybersecurity risk to our customers and network infrastructure is completely avoidable if the suggestions outlined below are taken.

Conclusion:

BIS must consider the impact the proposed regulations will have upon U.S. based organizations. Several suggestions to minimize impacts are: (1) Allow for intercompany transfers for items described on the Commerce Control List. A new license exception for intercompany transfers would be extremely helpful. A new license exception (ICT) would allow companies to transfer cybersecurity items and technology for internal use so that any immediate threats to our network infrastructure or vehicles can be immediately neutralized. (2) Make additional license exceptions available for use such as TSR, TSU, or LVS in order for U.S. based organizations to quickly respond to cybersecurity threats. (3) BIS could institute a fast-track licensing process whereby

intercompany licensing is reviewed and decided upon within a short timeframe (72 hours or less). While a fast-track process is not ideal, it would provide for more certainty that could be built in to our IT processes.

In addition to the most recent cyber-attack on the Office of Personnel Management (“OPM”) the Government Accountability Office has opined that “[s]ince fiscal year 2006, the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent.¹”

Cybersecurity preparedness cannot be overstated. Our network security teams have intercepted thousands of threats and more are coming. The proposed rules need to be rewritten so that U.S. companies are not prevented from securing vehicles and networks.

¹ CYBERSECURITY - A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges, Testimony Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, U.S. Senate. GAO-13-462T <http://www.gao.gov/assets/660/652817.pdf>

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-r6bg
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0130

Comment on FR Doc # 2015-11642

Submitter Information

Name: Matthew Joyce

Address:

8802 Ridge Blvd Apt D7

Brooklyn, NY, 11209

Email: matt@surly.bike

Phone: 9175969619

General Comment

As a technology industry professional having worked on formative developments in our industry at NASA and beyond, I've got a fairly significant investment personally in the area of Information Security. It is a desire amongst most technology professionals to ensure reliable and safer operations occur in any automation related endeavour.

The higher level goals of Wassenaar as they relate to information security are fundamentally laudable. However, the specific wording, and general tone are indicative of a very dangerous lack of contextual knowledge regarding several directly impacted fields of research, as well as existing workflows across most of the multi-trillion dollar US information economy.

The rise of exploit vendors and the trade of vulnerability information has put many organizations at risk. Well beyond the threat of international politics and military action, the simple fact is smaller boutique markets for this sort of information have begun to serve the needs of organized and not so organized crime. Scarcity is always a commodity and as complexity in attacks rises so too does the value of repeatable attack vectors. Sadly, the incentives that exist today for the handling of security research are almost entirely in the hands

of offensive pursuits, legal and extralegal. The workflows that had existed for addressing flaws as part of ongoing defensive and qualitative assurance measures have begun to suffer from this. A desire to reign in these new risks, and begin to provide some government oversight and / or enforcement is understandable.

However, the need for information research and development has never been greater. And that need is growing faster than exponentially at the moment. The push to automate and interconnect has branched out explosively across most logistical supply chains in all manner of industry. Securing those new infrastructures is of paramount importance. We face risks to life and limb from even unintentional failures, to say nothing of the malignant intentions of those who would bring harm to others. As part of the process of analyzing automation, mechanical or software, or even mathematical core principles... there is a need to develop, test, and share experimental platforms that do execute on theoretical flaws. We must continue to share the means to develop and deploy offensive resources. These resources are also the fundamental building blocks of quality assurance, and verification of safety. They are the crash tests of our industry.

While it is lamentable that very often our crash tests can be repurposed to ill intent, they are fundamentally, in the framework of development and quality assurance, the primary defence against aggressors, and the common 'bug'. And bug is as prescient a term today and in this discussion as it was when the term was coined. Squirrels are the chief threat to our nations power infrastructure today. They have caused the most amount of harm, by far. While intentional acts of sabotage remain a credible risk, squirrels are the proven masters of threat to that area of industry. Ensuring resiliency and security requires us to test the systems we produce. To test those systems we must deploy hazards and horrors upon those systems that are at the very forefront of R&D.

And more to the point, to remain agile, in the face of a demanding and global market, we must allow this testing to continue as it has in the manner that has proven best to date.

I wish to revisit the discussions that at the high level Wassenaar rules attempt to address. As I said, that discussion is important, and wanted by all if not most. However, the legislative actions suggested to date, remain a dangerous set of overly simplified and wide reaching measures. They are the products of minds that do not have a depth of grasp necessary to avoid the many pitfalls that beleaguer complex systems and those who design them as best they can. We wish to help. The volume of commentary speaks to that commitment from the industry. Allow us to provide you the context you need. To drive a part of the discussion necessary to the preservation of American supremacy in the information economy, and the quality and safety that that supremacy will be required of us by any natural or unnatural economic future we may breach.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-fy1m
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0131

Comment on FR Doc # 2015-11642

Submitter Information

Name: Brian Scarpelli

Address:

1320 North Courthouse Rd, Ste 200

Arlington, VA, 22201

Email: bscarpelli@tiaonline.org

Phone: 7039077714

Organization: Telecommunications Industry Association

General Comment

Please find attached comments from the Telecommunications Industry Association (TIA) in response to the May 20, 2015-published request for comment to inform BIS implementation of the Wassenaar Arrangement export control December 2013 Plenary agreements over cybersecurity items.

We urge you to reach out to the undersigned with any questions or concerns, or ways that TIA can be of assistance to BIS moving forward.

TIA is also filing this via publiccomments@bis.doc.gov.

Best regards,

Brian Scarpelli

Director, Government Affairs

Telecommunications Industry Association (TIA)

d: 703.907.7714 | m: 517.507.1446 | BScarpelli@tiaonline.org
TIAonline.org | Twitter: @TIAonline and @TIA_NOW

Attachments

TIA Comments - BIS Wassenaar Agreement Proposal 072015

**Before the
DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Washington, DC 20230**

In the Matter of)
)
Amendment of Parts 740, 742, 748, 772,) Docket No. 150304218-5218-01
and 774 of the Wassenaar Arrangement's)
2013 Plenary Agreements Implementation)
regarding Intrusion and Surveillance Items)

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7714

July 20, 2015

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY 1

II. GENERAL VIEWS ON ISSUES RAISED BY BIS PROPOSAL 3

 A. BIS Should Clarify Key Definitional/Scope Terms..... 4

 B. TIA Urges BIS to Avoid Unnecessary Restrictions on the Sharing of
 Information within and among Organizations 5

 C. Proposal to Require Sharing of Source Code for Licensed Items 6

III. TIA RESPONSES TO SELECT QUESTIONS POSED IN THE BIS REQUEST
FOR COMMENT 8

IV. CONCLUSION..... 10

**Before the
DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Washington, DC 20230**

In the Matter of)
)
Amendment of Parts 740, 742, 748, 772,) Docket No. 150304218-5218-01
and 774 of the Wassenaar Arrangement’s)
2013 Plenary Agreements Implementation)
regarding Intrusion and Surveillance Items)

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. Introduction and Summary

The Telecommunications Industry Association (“TIA”) hereby submits comments in response to the Department of Commerce Bureau of Industry and Security’s (“BIS”) request for comment to inform BIS’ implementation of the Wassenaar Arrangement (“WA”) export control December 2013 Plenary agreements over “cybersecurity items.”¹

TIA represents hundreds of ICT manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the critical infrastructure sectors directly impacted by the BIS proposal. Representing our membership’s commitments in this area, TIA also holds membership and is actively engaged in key public-private efforts that contribute to secure information systems,

¹ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853 (May 20, 2015) (“BIS Proposed Rule”).

including the CSRIC; the Communications Sector² and Information Technology Sector³ Coordinating Councils; and the National Coordinating Center for Communications (“NCC”), the Information Sharing and Analysis Center (“ISAC”) for telecommunications, part of the Department of Homeland Security’s (“DHS”) National Cybersecurity and Communications Integration Center.⁴

Through its Cybersecurity Working Group, TIA members engage in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments should provide more timely and detailed cyber intelligence to industry to help identify threats to protect private networks.
- Cybersecurity funding for federal research efforts should be prioritized.

TIA appreciates BIS’ efforts to create a transparent and inclusive multistakeholder process to address key cybersecurity challenges and looks forward to working with the BIS and other governmental stakeholders, both directly and through the envisioned multistakeholder process moving forward. In comments below, TIA:

- Urges BIS to provide needed definitional clarifications;
- Urges BIS to avoid unnecessary restrictions on the sharing of information within and among organizations;

² <http://www.commscc.org/>

³ <http://www.it-scc.org/>

⁴ <http://www.dhs.gov/national-coordinating-center-communications>

- Provides input on the proposed ability of BIS to require source code from newly-covered items under this WA expansion; and
- Provides answers to select questions posed by BIS related to the impact of the proposal.

II. GENERAL VIEWS ON ISSUES RAISED BY BIS PROPOSAL

Initially, TIA notes that it shares the WA's goal of improving regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulation and use by bad actors. Further, TIA appreciates the importance of the concerns underlying the WA regarding the production, export, and utilization of weaponized software. However, many of the techniques used by attackers through this software are important to defenders seeking to test their defenses against intrusion. Therefore, TIA strongly urges BIS to move forward only after careful consideration of and deliberation on the views of impacted shareholders before implementing the WA.

TIA has long urged the United States government that it should not enact policies within the United States which would unduly restrict trade in ICT equipment and software. Across numerous contexts, other countries have cited similar concerns regarding foreign ICT equipment and are currently considering overly-broad and/or overly-restrictive trade measures. If these countries adopt such policies, the United States' global economic competitiveness could be severely adversely affected. TIA urges BIS to recognize that the success of the United States' ICT industry depends upon a global development model.

The global ICT industry relies upon a flexible supply chain that is characterized by intense competition, price fluctuation, and supply of different inputs. Since hardware and software products and components may be designed, aggregated, tested, and finalized in different locations, it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. Therefore, the focus of any product security concerns must always be on whether the product is secure, not on the country of origin. It is frankly unrealistic to expect that all of the resources necessary to secure complex networks will reside inside of one country.

Further, in the interest of protecting innovation from technologically discriminatory policies and regulations, TIA strongly urges BIS to remain true to the principle of technological neutrality. While it is important for the United States to honor its commitments and help ensure greater international security, it must not do so at the expense of the critical technological advantages created and enjoyed by the innovative freedom and spirit of the ICT industry.

A. BIS Should Clarify Key Definitional/Scope Terms

TIA believes that definitional clarity is crucial to the successful discussion or implementation of any regulatory regime. Any uncertainty could lead to hesitation and, potentially, greater market disruption. These disruptions can manifest as increased use of resources on legal compliance, licensing fees, etc., rather than research and development. For example:

- While BIS has noted that Category 4 control entries would govern “the command and delivery platforms for generating, operating, delivering, and communicating with ‘intrusion software’” as well as “the technology for developing ‘intrusion software,’” the rules would not cover “intrusion software” itself.⁵ As a result, “transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware” would not fall under the BIS controls.⁶ In reviewing the proposed BIS rule, TIA fears that, in practice, making a distinction between the “platform” for the intrusion software and the intrusion software itself will be intensely difficult. For example, because companies that develop software for products and services require the use of basic tools such as operating systems (and hardware compatible with those operating systems), these basic tools could be interpreted as falling under the BIS rule. We do not believe such a wide scope to be in the interest of the WA and urge for BIS to engage with stakeholders towards providing further written clarity on this aspect of the proposal before any new export requirements are finalized.
- TIA urges for BIS to more clearly define the meaning and scope of “communication with” intrusion software means.⁷ Based on the BIS proposal, TIA believes this key term to be over-inclusive, and impacted organizations are likely to have difficulty determining the limits of this term.

⁵ FAQ

⁶ *Id.*

⁷ BIS Proposed Rule at 28554.

- As another example, the BIS proposal would extend over “Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor.”⁸ TIA members use IP network communications surveillance to track, anticipate, and counteract intrusion software attempting to breach their systems. As proposed, BIS would be inserting itself into, and impeding, this essential and widely-used network security practice. TIA believes that this aspect of the BIS proposal should be as narrowly scoped as possible to address BIS’ interests without harming basic network security management for the private sector through revisions to make clear that the rule will not impact companies’ ability to monitor their own networks to detect and mitigate nefarious intrusions.

B. TIA Urges BIS to Avoid Unnecessary Restrictions on the Sharing of Information within and among Organizations

BIS proposes that all exports of specified systems, equipment, components or software that would generate, operate, deliver or communicate with ‘intrusion software’ would require an export license under the proposed rule.⁹ Notably, BIS has also stated that, as proposed, the new WA rules contain “no license exception for intra-company transfers or internal use by a company headquartered in the United States under the proposed rule.”¹⁰

As noted above, in an era of globalized ICT development and sales, countless TIA members conduct tests on both hardware and software at locations around the globe. TIA believes that, as proposed, this aspect of the BIS proposal would place licensing requirements (or, at minimum, a need for the seeking of exemptions) on a nearly endless amount of company internal transactions that are necessary in the development of hardware and software products and services. If ICT companies in the United States were forced to gain approval for every single test performed outside of the United States, as is implied by this definition, the security of American business would, inevitably, be severely undermined. The impact of this policy would place significant resource and time delays into the product development cycle where intra-

⁸ *Id.*

⁹ BIS Proposed Rule at 28854. Term used is “Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices”

¹⁰ <http://www.bis.doc.gov/index.php/policy-guidance/faqs>

organization software development teams share information, collaborate on code development, and distribute work product. In short, TIA believes that the lack of an exception in the BIS for intra-company transfers or internal use will present an untenable environment for companies that develop network security products and services, and we urge BIS to further engage with stakeholders towards a revised, and more feasible, application of the WA.

Furthermore, TIA notes that BIS proposal in this context may conflict with established Federal policy regarding the sharing of cybersecurity threat information among key stakeholders, both public and private. The United States government, in partnership with industry members from across critical infrastructure sectors, remains committed to the sharing of timely cybersecurity threat information through the NCCIC/Comm-ISAC (see above). In the last few years alone, the Administration has undertaken a number of important activities to improve cyber defenses, enhance response capabilities, and upgrade incident management tools in both the private and public sectors.¹¹ As just one recent example, Executive Order 13691 took steps to improve the sharing of timely cyber-based threat information amongst and between government and industry stakeholders through the establishment of Information Sharing and Analysis Organizations (“ISAOs”).¹² TIA, along with countless other public and private stakeholders, strongly believes that as the number and diversity of cyber threats to both the public and private sectors continue to increase, it is more important than ever for the enablement of voluntary real-time bi-directional sharing in any way possible. The impact of this BIS proposal clearly complicates, thereby impeding, this information sharing by forcing licensing requirements and associated liability concerns into the process. BIS is encouraged to closely coordinate with other Federal stakeholders as well as industry to ensure that the collaborative environment being striven for is not disrupted.

C. Proposal to Require Sharing of Source Code for Licensed Items

As written, BIS would, upon request, be able to demand that the licensing applicant include “a copy of the sections of source code and other software (e.g., libraries and header

¹¹ See, e.g., <https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015>

¹² See Exec Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing (February 13, 2015), available at <https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing> (“EO 13691”).

fields) that implement or invoke the controlled cybersecurity functionality.”¹³ Across contexts, TIA strongly opposes proposals that would require the escrowing of source code in order to gain access to markets. Product source code represents the highest level of business confidentiality for the ICT industry, and requiring the disclosure of these codes is a strong incentive not to invest in crucial research and development. Further, such a policy may have the impact of forcing the movement of development teams to locations outside of U.S. jurisdiction to avoid this policy. While TIA understands that requiring source code of some encrypted items is an existing requirement under BIS rules implementing the WA, we strongly urge BIS not to extend this requirement to items contemplated under this rulemaking.

Sovereign interest in a secure and development-friendly cyber economy is best served, in any country, by policies that encourage competition and customer choice. In numerous contexts internationally, TIA members continue to face anticompetitive proposals that include mandatory escrowing of source code. We strongly urge BIS to ensure its proposals are consistent with established USG policy, and to contemplate the impact such a policy would have on other governments that look to the United States as an example of prudent regulatory behavior. Further, TIA requests that BIS clearly justify why it would need to review such business confidential information to accomplish their goals under the WA.

¹³ BIS Proposed Rule at 28855.

III. TIA RESPONSES TO SELECT QUESTIONS POSED IN THE BIS REQUEST FOR COMMENT

- a.** *How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:*
1. *How many additional applications would be for products that are currently eligible for license exceptions?*
 2. *How many additional applications would be for products that currently are classified EAR99?*

Due to the sweeping expansion proposed by BIS, many companies should expect to see a significant increase in the number of licenses based on the requirements under the proposal as written. As described above, the impact of this proposal would interfere in all phases of product development, from the initial stages of research and development to the shipment of final products. For larger companies, the increase in needed licenses could be in the thousands.

- b.** *Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.*

Based on the wide reach of the definition of "intrusion software," the BIS rule as proposed would have profoundly negative effects on legitimate vulnerability research, audits, testing, and screening of company networks as well as those of their clients. As noted above, due to the global nature of the ICT industry, many tasks required by vulnerability assessment teams would potentially require licenses on a per-communication basis, not only for those developing "intrusion software," but also for those developing or using a system that "communicates with" intrusion software.

In addition to governing transactions across geographic borders, the proposed BIS rule would implicate transactions within a single room should one of the employees be of a nationality other than the U.S. or Canada. The interruptions and costs associated with implementing BIS' proposal would not only reduce the ability of companies to invest and

innovate, but would also result in delayed mitigation of network vulnerabilities that are identified. It is crucial that BIS refrain from interfering in the intra-organizational development of network intrusion tools and products. In addition to the impact of the companies seeking the license themselves, the BIS proposal would also have a similar trickle-down effect on trusted third-party contractors, whether in the product development cycle or in a post-deployment security audit.

We note that the BIS proposal runs counter to the existing public-private partnerships used across critical infrastructure sectors to share timely cybersecurity threat information. Finally, TIA wishes to underscore the negative example the proposed approach would set in the international community where the private sector continually contends with country-specific discriminatory economic policies.

IV. CONCLUSION

Based on the concerns listed above, we believe that the stated intent of the proposed regulations appears significantly different than the scope of the actual requirements. We look forward to working with the Department of Commerce to ensure that the goals of the proposal can be met in a manner that are narrowly tailored to the actual risks faced by our nation.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7700

July 20, 2015

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-zj05
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0132

Comment on FR Doc # 2015-11642

Submitter Information

Name: Todd Jarvis

Address:

1325 Howard Avenue

Suite 253

Burlingame, CA, 94010

Email: todd@packetstormsecurity.com

Phone: 408-891-9551

Organization: Packet Storm Security

General Comment

To whom it may concern,

I appreciate you taking time to read this response to your software modifications to the Wassenaar Arrangement.

I come to you as a 20 year veteran of the information security industry and as an owner of one of the largest online information portals for this field. It is free to all, globally, and is heavily leveraged by governments, corporations, and researchers. Our purpose is to provide up-to-date security information and relevant news with regards to new flaws in software. We also provide free tools donated from all over the Internet. Some open source, some not. This is inclusive to what you label as intrusion software and zero day exploits. We "internationally export" "intrusion software" and exploits on a per-second basis. To put into perspective how important our resource is, the United States Army once requested a live mirror of the system in order to train their troops. We receive no revenue from providing this service, so I have no objection to

your additions based upon an impact to our business.

I point all of this out because your proposed rules will force us to close our doors and in turn affect everyone's security, including national security. Over the past 15 years, many government officials have thanked me personally for keeping this resource alive and that it was a necessary tool for them to do their job. The ambiguity of this new proposal makes our ability to maintain this system untenable.

Your suggested verbiage in this act implies that zero-day exploits will need licensing and export controls. You also employ tight regulations around the ambiguously titled "intrusion software".

In your FAQ, you claim that the proposed rule would not control any intrusion software ("1. Does the rule BIS is proposing control "intrusion software", malware, exploits, etc.?"") but then, further down, says you would control information required for developing, testing, refining, and evaluating "intrusion software" and technical data to create a controllable exploit. ("4. Will the rule control vulnerability research as well as research on exploits?")

Which is it?

If the latter, are you now making all operating systems illegal? What about compilers?

Ambiguity around such a sensitive topic can only stifle open discussion with regards to vulnerabilities. The result is that researchers will stop these discussions out of fear, and in turn commercial products that you depend on to protect your network will no longer be effective as they depend on the very same security community to function. It's an ecosystem. A very fragile ecosystem.

Hackers who swap exploits and "intrusion software" will continue to do so regardless of your proposal, and their effectiveness will be strengthened if the security community cannot work to protect you against these attacks.

I believe the intentions of the BIS are meant to be positive, but are unfortunately very misguided. My plea is that you please immediately remove all restrictions surrounding exploits, "intrusion software", and cryptography before you trigger a catastrophic domino effect that impacts billions of lives.

Thanks for reading.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-33h1
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0133

Comment on FR Doc # 2015-11642

Submitter Information

Name: Bas Alberts

General Comment

To be able to legislate something you have to be able to define what that something is. "Exploit" is just shorthand for "input into an algorithm that triggers certain states within that algorithm, where such states have an adverse security impact on the environment implementing the algorithm".

Simply put: exploits are just input into algorithms.

So having defined what an exploit is, this would imply that BIS would need to establish a regulatory body that decides whether or not a certain input generated by a piece of software may or may not trigger publicly known or unknown (i.e. Oday) adverse security states in a receiving algorithm.

E.g. sending a 1 to web application A may allow authentication bypass, whereas sending that same 1 to web application B may trigger completely legitimate protocol interaction. When is an input of 1 an exploit? That would depend on context of use right? A gun is a gun, but a 1 is symbolic and can mean many things which makes it extremely difficult to attach legally binding definitions to.

So trying to define when input is or isn't an exploit is, by definition, at worst a paradox and at best highly context dependent. Which makes implementing legislation that controls something as undefinable and paradoxical as "an exploit" ambiguous. Such ambiguity then leaves

enormous potential for abuse and misappropriation by allowing for gross governmental overreach and extension to any and all software.

This in turn fundamentally encroaches on the principle of symbolic free speech, under which source code should be protected as well.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k35-hkv2
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0134

Comment on FR Doc # 2015-11642

Submitter Information

Name: Justin Malyn

Address: United States,

Email: malynj@umkc.edu

Phone: 816-235-5294

General Comment

The addition of rootkits and exploit code to the list of Wassenaar controlled items will cause a chilling effect in regards to vulnerability testing of commercial software products. Commercial software products, such as Adobe Flash, inherently have vulnerabilities. If security research communities fear running afoul of the Wassenaar agreement, they may stop providing information that is critical in patching and fixing these security issues.

Intrusion detection systems should be removed from the Wassenaar agreement. Some of these systems, such as a product known as Snort, are open source and benefit greatly from community input into new detections that security researchers world wide provide. Restricting these systems will reduce the number of researchers who will contribute to these open source detection systems, and will reduce the effectiveness of this open security platform. This will also affect closed-platform systems, as many of these will adapt detections made to the open source systems into their own close systems. The net effect is that non-participating countries will not actively contribute detections, and may develop variants of the existing systems, resulting in significant fragmenting of this specialty area of network security.

The risk of both of these items, is that security companies will setup outside of the Wassenaar agreement countries, in order to avoid their products and services being export controlled. This

would reduce the security talent pool in participating countries, and lower the security of participating countries as major advances begin to occur in products produced external to these countries.

Companies such as Microsoft and Adobe will also find themselves unable to pay finder fees (bug bounties) to security researchers in non-agreement countries, as those researchers would be less willing to have the information they discover turned over to Wassenaar participating countries and subsequently controlled. These researchers would be more likely to sell discovered items to larger security companies outside of the Wassenaar agreement countries.

PUBLIC SUBMISSION

As of: July 27, 2015 Received: July 20, 2015 Status: Posted Posted: July 27, 2015 Tracking No. 1jz-8k35-q8jn Comments Due: July 20, 2015 Submission Type: Web
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0135

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous foreigner

General Comment

A response to the proposed rules from BIS from a foreigner

Computer security is becoming an increasingly important issue these days, with large scale hacks and billions of new devices coming online.

The real defense against malicious hackers is more secure ("hardened") systems, a point stated by most experts in computer security (ex: Matt Blaze at the university of Pennsylvania). Legislation has its place, but no law can keep a boat full of holes afloat.

Even vendors who used to shy away from discussing vulnerabilities in their products (due to reputation issues) are slowly warming up to this fact, with the rise of bug-hunting programs ect. The perception of refusal to admitting and doing something about insecurity is becoming increasingly costly.

THE EFFECT ON BASIC RESEARCH:

The international security research community forms a defensive barrier for the internet against bad actors and they work in a highly organic way with lots of cross-border information sharing.

The new proposal would hamper the information flow and deincevitize security work due to

potential legal risks, the hassle of licensing applications and so fourth, an opinion shared with many experts in the field. Diminished output of basic research will have negative consequences when the number of systems increases along with the number of attacks, while the output of research that keeps these systems safe cannot keep up.

THE EFFECT ON DAY2DAY DEFENSIVE CAPABILITY:

Diminished output from basic research will lead to less potent defensive security tools, while criminal actors still having access to many avenues to get the same techniques the basic research fails to deliver.

Without ongoing offensive security testing (testing your network using "hacker tools"), it's almost impossible to attain a high degree of security. Not having full access to these tools and/or weakened versions as the proposed rules hints to means playing with a blindfold against an attacker able to see all that's going on.

Most experts will tell you this!

As a result: Attackers gets more direct power, defenders gets less power. Highly unethical if preventable and hardly the result we want.

THE EFFECT ON VULNERABILITY PROGRAMS:

Reluctant vendors are warming up to working with the security community to reveal vulnerabilities and winwin collaborations are being created. Creating completely secure and reliable code is a problem that has not been solved (even NASA can't do it after 4+ decades of trying!) and as a result products ship with lots of vulnerabilities. Finding and fixing them has become a race between actors of good and bad intentions, and the best policy is to help the "good side" to do this as efficiently as possible as the bad actors will do it anyway. These new rules only create barriers for the "good guys".

THE PROBLEM OF ENFORCEMENT:

Enforcing laws in the cyber-domain is extremely difficult. On top of this the rules are written so vague that they might allow for selective enforcement, and if history repeats itself, selective enforcement will occur if the law allows it.

A potential outcome of this could be a high degree of injustice for a selected few who only tried to help, while putting others at risk because the researchers being unjustly treated never got to share their findings.

IMPACT ON THE US:

Mistrust towards american IT (in general) has exploded the last few years with the surveillance exposures and to a lesser extent with the latest initiative against encryption.

Passing this proposal in its current form, in spite of enormous backlash from the security community and wider IT industry could enhance this mistrust even further.

Questions like: "Who benefits from these rules?" and "Why do they seem to deliberately disfavor cyber-security (especially in light of the recent OPM hack)?" frequently comes up in discussions about the US overseas.

Couple this with the fact that these proposals could give american IT organizations worse defensive capability internally hardly helps improving the eroding trust in American IT services.

Why would anyone buy from the US given the disregard for security and potential practical difficulties for US companies in using security tools that actually work to keep customers secure?

As a final note on the mistrust issue: It's one thing to pass this given the severe warnings from the security community.

It's another thing completely if this proposal passes in its current form leading to REAL security issues instead of hypothetical ones.

This would not only damage the US reputation for cyber security and privacy tremendously, but it would hurt people, industry and the american economy.

To conclude: Given the original intention of these proposed rules, please reconsider the proposal and work with the ecosystem of security researchers around the world trying to keep us safe.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k36-cmam
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0136

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

As I'm sure others have already pointed out, the regulations won't work. In general I'm behind the *spirit* of the regulation, but it simply is too broad. If you start covering *research*, you will close down our 6 month-old startup. Because we, like everyone else in the industry, have to use offensive research to promote our skills. Defensive research will almost never get you a speaking spot at a conference.

If regulation is to be applied anywhere, it should be focused on the actual root cause of the entire need for a security industry - the externality that allows companies to make software and not be accountable for its shoddy construction causing billions of dollars in harm to their customers. We used to not have building regulation. And then people got burned (literally.) People's IP, and bank accounts, and livelihoods are getting burned every day due to software vulnerabilities. That is what should be focused on if you want to actually make a difference.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k36-v0sh
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0137

Comment on FR Doc # 2015-11642

Submitter Information

Name: Ingrid Skoog

General Comment

I have worked in the information security field for over 10 years. I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

I recommend the DoC suspend its current implementation of the additions to the Wassenaar Arrangement. A more thorough investigation of the stakeholders and potential impact must be made to ensure the needs of the USG in implementing such an arrangement does not hinder the valuable work of our security community.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k37-82o2
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0138

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

As a top 1% infosec researcher who has found numerous critical XSS bugs over the last few years, I am absolutely appalled at this proposed legislation. I'm willing to bet my OSCP certification that more than half of you fools don't even understand what this stuff means. Leave the cybersecurity industry to the pros please.

Signed,

- /r/AskNetsec

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k37-zzwu
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0139

Comment on FR Doc # 2015-11642

Submitter Information

Name: Kevin Johnson

Address:

283 Concord Ave.

Lexington, MA, 02421

Email: kjscreen-fedreg@yahoo.com

Phone: 781-863-1186

Organization: Self

General Comment

A virus or malware is different from most controlled items because it can be neutralized once disclosed. The potential of the license approval process to slow the export of virus testing solutions suggests that a disclosure requirement should be adopted first, rather than a license requirement.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k37-iszv
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0140

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Osborn

Address:

Goodwin Procter LLP
901 New York Avenue NW
Washington, DE, 20001

Email: josborn@goodwinprocter.com

Phone: 202-346-4133

Fax: 202-346-4444

Organization: Offensive Security

General Comment

See attached file(s)

Attachments

Offensive Security Comments to Proposed Intrusion Controls Rule FINAL



Offensive Security’s Comments to “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items,” 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63.

Offensive Security Services LLC, a Delaware corporation that performs security-assessment services and provides information-security related training, and OffSec Ltd, a Cayman corporation that maintains community-based open-source software projects to assist in professional security testing (collectively, “Offensive Security”), hereby submit these comments to the rule proposed by the Bureau of Industry and Security (“BIS”) involving the control of intrusion-delivery software. *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63 (“Proposed Rule”). Offensive Security strongly opposes the Proposed Rule and believes its promulgation without significant amendments would provoke consequences that are unintended and ultimately detrimental to the U.S. national security and to the viability of the U.S. penetration-testing industry.

In Part I below, Offensive Security introduces its business and the software, technology, and services relied upon by its customers for network and system security. In Part II, Offensive Security explains why it believes the Proposed Rule would: (i) damage Offensive Security’s business and other U.S.-based businesses operating in the security space; (ii) have a detrimental effect on cybersecurity and preventing cyberattacks worldwide; and (iii) be ineffective as a means to thwart malicious actors — including human-rights abuses abroad — who use intrusion software for offensive and malicious purposes. In Part III, Offensive Security recommends modifications to the Proposed Rule that would alleviate the concerns expressed in Part II. And, in Part IV, Offensive Security provides responses to the specific questions posed by BIS. *See* Proposed Rule at 28,856.



I. Offensive Security’s Business and Offerings

Offensive Security was founded in 2007 on the belief that the only way to achieve sound defensive security is through an offensive approach. The Offensive Security team is comprised of security professionals having extensive experience attacking systems to determine how they respond in order to take appropriate defensive measures. The Offensive Security team shares its collective security knowledge and industry expertise with interested members of the public through trainings, free tools, and publications. Operating under the motto “Try Harder,” the Company’s trainings and certifications are well-respected and considered amongst the most rigorous available, creating a model embraced across the industry. These trainings and certifications are utilized by thousands of companies worldwide to train their IT and security professionals.

In addition to its training and certification offerings, Offensive Security offers various open-source, publicly available community projects such as the Exploit Database, Metasploit Unleashed, and Kali Linux (previously BackTrack Linux). These community projects are highly-regarded and used by security teams in governmental and commercial organizations across the world. For more information about Offensive Security and its offerings, please visit www.offensive-security.com.

As one of its open-source community offerings, Offensive Security provides Kali Linux¹, the industry *de facto* standard open-source Linux penetration-testing platform. Kali Linux is used industry-wide by government, commercial organizations, and hobbyist to learn about information security matters, and to identify and exploit systems to further secure them by fixing the identified issues. Kali Linux is made publicly and freely available. Offensive Security is committed to supporting the open-source community with the ongoing development of Kali

¹ Available for download at <https://www.kali.org/>



Linux. The development tree and all source code for Kali Linux are available for those who wish to tweak and rebuild packages.

As another of its community offerings, Offensive Security provides the Exploit Database.² The Exploit Database is a “CVE compliant” archive of public exploits and corresponding vulnerable software, maintained for use by penetration testers and vulnerability researchers worldwide. Because the Exploit Database is “CVE compliant,” all of the exploits made available in the Exploit Database are also submitted to the Common Vulnerabilities and Exposures dictionary of publicly known information-security vulnerabilities and exposures (“CVE List”). The CVE List is maintained by the Mitre Corporation and sponsored by the Office of Cybersecurity and Communications, U.S. Department of Homeland Security. The purpose of the CVE List is to provide common names for publicly known cyber security issues, and make it easier to share data across separate vulnerability capabilities with the common enumeration. The CVE List feeds the U.S. National Vulnerability Database (“NVD”), which then builds upon the information included in CVE entries to provide enhanced information for each CVE Identifier such as fix information, severity scores, and impact ratings. NVD also provides advanced searching features such as by individual CVE-ID; by OS; by vendor name, product name, and/or version number; and by vulnerability type, severity, related exploit range, and impact.

The Exploit Database is thus a tool that provides known exploits to security and vulnerability researchers. Its aim is to serve as the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proof-of-concepts rather than advisories, making it a valuable resource for those who immediately require actionable data. The Exploit Database is a non-profit project that is provided as a public service by Offensive Security.

² Available at <https://www.exploit-db.com/>.



As described above, Offensive Security provides multiple information-security training courses. Penetration Testing with Kali Linux (“PWK”) is an information-security training and ethical hacking course. This course is designed for network administrators and security professionals who need to acquaint themselves with the world of offensive security. This penetration-testing training introduces the latest hacking tools and techniques in the field to simulate a full penetration test from start to finish. Cracking the Perimeter (“CTP”) takes all of the skills acquired in the PWK course and further hones them by exposing students to an extremely challenging lab environment developed using actual scenarios faced by the Offensive Security team during live penetration tests. During the CTP course, students are given an in depth examination of the vectors used by today’s attackers to breach infrastructure security.

The Offensive Security Wireless Attacks course (“WiFu”) teaches students the basic concepts of wireless networking and builds upon that foundation to conduct attacks against wireless networks of varying configurations. Relevant not just to penetration testers, WiFu is highly recommended for anyone responsible for configuring and securing wireless networks. By understanding how wireless networks are attacked, administrators will know how best to protect their own wireless infrastructure.

The most demanding course provided by Offensive Security is the Advanced Windows Exploitation course (“AWE”), featuring a sophisticated hands-on computer lab environment challenging students to bring out their best penetration-testing skills. The case studies covered during the AWE course include public vulnerabilities and vulnerabilities discovered by the Offensive Security research team, all of which cover a wide range of applications and exploitation techniques.

Offensive Security provides industry-leading information-security certifications which are considered the most rigorous test of skill available in the computer security field. These performance-based certifications are based entirely on demonstrated ability and merit.



Many employers throughout the country rely on these certifications for determining the technical qualifications of security professionals applying for employment in the industry.

For each of the certifications, Offensive Security does not rely on outdated multiple choice based questions. Instead, candidates are presented with a series of real-world hacking tasks that they must complete in a limited amount of time. Pass or fail is based on candidate performance.

Offensive Security additionally provides advanced security-consulting services to government agencies and the private sector. These consulting services are conducted by creating a simulation of the target environment and modeling identified attack points. As part of its comprehensive consulting services, Offensive Security may develop custom attacks that are specific to the target organization's network, software, and systems. For any given organization, a unique combination of software and work-flow creates targets of opportunity that are often overlooked or impractical to attack using traditional assessments methods. Hence, Offensive Security may deliver a series of customized attacks to ensure a complete security assessment.

As part of its consultation services, Offensive Security may create new attacks or modifying existing attacks based on differences encountered in the real world compared to the lab environment. After developing a customized attack, Offensive Security is able to actively simulate a determined attacker that has specifically targeted the organization. These custom attacks will often times contain exploits that are unknown by a third-party software vendor or unpublished. Once these new vulnerabilities are discovered by Offensive Security, however, the vulnerabilities are then provided to the respective software publishers for them to develop and release a patch or update in order to increase the security of the third-party vendor.

When finished developing a customized attack and simulating in the real-world, Offensive Security provides an application-security assessment to its customers. These



application-security assessments include the results of software-application testing, which is a crucial part of any security audit.

In Offensive Security’s experience, organizations across the world often face difficulty in finding a security team of experienced analysts to conduct a high quality, intensive, and non-automated application-security assessment. Offensive Security has built a strong reputation in vulnerability discovery, exploit development, and securing networks and systems, as well as teaching others how to do the same for a number of years. The experienced Offensive Security team conducts in-depth vulnerability analysis of target applications. The assessments are conducted using various methodologies including reverse engineering, protocol analysis of legitimate traffic, protocol fuzzing, and manual traditional and custom attacks against the exposed attack surface. Once the application-security assessment is complete, Offensive Security delivers a comprehensive report, including highly detailed and chronological descriptions of all discovered issues. In some cases, these reports may include information about custom-developed exploits used to demonstrate discovered vulnerabilities, as well as video presentations of those exploits in action. The exploits discovered by Offensive Security may be unknown and unpublished exploits (thus far), but when made known by Offensive Security, software vendors may use the exploits to improve product security.

In sum, the business of Offensive Security is to educate and train security professionals across the world in order to create a strong defensive cyber security environment.

II. Negative Impact of The Proposed Rule

For Offensive Security’s customers, the security needs addressed by our products and services are both critical and incessant. Daily news headlines depict public and private-sector actors under constant cyberattack. As a recent example, on July 9, 2015, the federal government announced that 22 million people were affected by cyberattacks on the Office of Personnel Management, leading to loss of social security numbers and other personal, financial



information.³ The cyberattack on OPM was reportedly linked to the Chinese government. On the commercial side, Home Depot, the world’s largest home improvement retailer, announced in November of 2014 that credit card and personal data for some 53 million users were stolen during a breach.⁴ According to Home Depot, the breach involved the use of custom-built malware installed on Home Depot’s self-checkout systems. *Id.* These are but two recent examples of many.

The offensive use of intrusion-delivery software also raises human-rights concerns. For example, Egyptian dissidents who ransacked the offices of Egypt’s secret police following the overthrow of Egyptian President Hosni Mubarak discovered a contract with a third-party to use the FinFisher spyware software to spy on Egyptian citizens and political adversaries.⁵ As another example, in 2014 an American citizen alleged the Ethiopian government had surreptitiously downloaded FinFisher on his computer and was using the spyware to wiretap his private Skype calls and monitoring his family’s use of the computer over the period of a few months.⁶

For these and other reasons, the government, public, and business communities in the United States and among our global friends and allies have a shared interest in ensuring that malicious software is not obtained by malicious actors or used maliciously — indeed, never has the need for protection against these sorts of cyber intrusions been more acute than it is today. But this is precisely why it is vital to maintain and encourage U.S. dominance in this space, and

³ Nakashima, Ellen, “Hacks of OPM databases comprised 22.1 million people, federal authorities say,” *The Washington Post* (Jul. 9, 2015).

⁴ Press Release, The Home Depot, “The Home Depot Reports Findings in Payment Data Breach Investigation,” (Nov. 6, 2014).

⁵ Leyden, John, “UK firm denies supplying spyware to Murbark’s secret police,” *The Register* (Sept. 21, 2011).

⁶ Cardozo, Nate and Cohn, Cindy, “American Sues Ethiopian Government for Spyware Infection,” *Electronic Frontier Foundation* (Feb. 18, 2014).



to ensure that *defensive* products, services, and technology, such as those offered by Offensive Security, are available for use in protecting enterprises, government, and individuals. The Proposed Rule threatens to cripple this industry in the United States, driving it offshore and, ultimately, outside of the reach of U.S. jurisdiction and regulation, as we now explain.

A. The Proposed Rule Would Damage Offensive Security’s Business and Other U.S. Businesses

Although the majority of the penetration-testing software and training materials utilized by Offensive Security during its security consultations are based on open-source, publicly available tools (such as Kali Linux) and thus not “subject to the EAR” under 15 C.F.R. § 734.3(b)(3), as explained above, Offensive Security is at times requested to customize training materials, exploits, and tools in order to provide its students with the most comprehensive training and its customers with the most comprehensive security audit information. Thus, at least some of the training, software, and services provided by Offensive Security would potentially involve “technology” meeting the criteria of 4E004 and perhaps software meeting the criteria of 4D004 as specially designed or modified for the generation, operation or delivery of, or communication with, intrusion software.

As explained by the Proposed Rule, Regional Stability (“RS”) controls would apply to U.S.-origin intrusion-delivery technology and software, and would thus require a validated license for export to all foreign countries other than Canada. Because this important information is necessary to both train students on how to become competent security testers, as well as to communicate both to and from Offensive Security’s customers in developing custom security testing, the Proposed Rule threatens to undermine Offensive Security’s business in a very material way. In part, the Proposed Rule would eliminate Offensive Security’s eligibility for important license exceptions found in License Exception ENC — indeed, other than a limited GOV license exception for exports to U.S. government entities abroad, there would be no license exception available for Offensive Security’s controlled technology and software.



The Proposed Rule threatens to damage or eliminate Offensive Security’s ability to provide U.S.-origin training services outside of the United States and to non-U.S. citizens, as well as consulting outside of the United States and within the United States to non-U.S. persons. This may include services and technology provided to the foreign branch offices and foreign subsidiaries of iconic U.S. companies; to NATO allies; and to multinational companies whose networks house data belonging to U.S. companies or the protection of which is otherwise vital to the U.S. national security. Offensive Security agrees with many other industry leaders who are submitting comments to the Proposed Rule that, in the name of denying offensive tools to bad actors intent on doing harm to the United States, the Proposed Rule would deny to these and other legitimate organizations the critical training and tools necessary to defend themselves against cyberattacks.

The Proposed Rule would, at a minimum, create unworkable internal training and software-development impediments for Offensive Security, limiting our ability to employ or engage non-U.S. citizens, since it would require us to apply for “deemed export” licenses. Thus, predictably, the U.S. domestic provision of training services and development of defensive cybersecurity tools will fall behind, as foreign talent in this space will become harder or perhaps impossible to enlist. These limitations will strike hard at Offensive Security, whose collective non-U.S. person workforce is roughly 85% of its total. Given the ambiguous demarcation between controlled and non-controlled technology (even under the most painstakingly worded regulations in the EAR), it could be impractical and perhaps impossible to cabin its non-U.S. workforce to only non-controlled software and technology. Thus, even as we face a proliferation of threats from abroad, we will become an inward-looking domestic industry. We will lose our effectiveness, to the ultimate detriment of the U.S. national security and industrial base.

Many other U.S. businesses are likely to be similarly affected and competitively disadvantaged vis-à-vis security firms providing non-U.S. origin training, software, and technology. To provide training, services, and technology, the administrative burdens, cost, and



delay involved in seeking licenses for instructors, students, and foreign customers would be detrimental to U.S. industry. Significant time, costs, and legal fees would be required to understand and comply with the license application process for each non-U.S. instructor, student, customer, and employee.

Offensive Security also agrees with other commenters to the Proposed Rule that the Proposed Rule will present an uneven playing field for U.S. companies vis-à-vis foreign competitors. An obvious consequence of the Proposed Rule is to hand to non-U.S. producers of course materials and intrusion-delivery technologies a critical and perhaps decisive distribution advantage over U.S. firms. Although each signatory to the Wassenaar Arrangement has committed to controlling intrusion software and technology, none appears to have adopted anything approaching the level of restriction in the Proposed Rule. For instance, the European Union has implemented minimal controls to intrusion-delivery software and technology by adding the item to Annex I to Regulation (EC) No. 428/2009.⁷ Except for a subset of Annex I items designated for stricter controls and listed in Annex IV, the transfer of items within the EU community requires only that exporters maintain records for at least three years, and indicate on commercial documents that the items are subject to further controls if exported from the EU community.⁸ The vast majority of Annex I items, including intrusion-delivery software and related technology, may be traded freely — without registration or licensing — within the EU community.⁹ Exports from EU Member States to seven “friendly countries” — Australia,

⁷ See Commission Delegated Regulation 1382/2014, at 13, 130-31, http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf.

⁸ See Council Regulation 428/2009, Annex IV, pp.260-66, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF>. Annex IV includes military, cryptologic, and chemical-weapons related items that are subject to additional restrictions, even when transferred within the EU community. See also Council Regulation 428/2009, Ch. VIII, art. 22(1), p.9; Ch. VIII, art. 22(8) p.10; Ch. VIII art. 22(10), p.10.

⁹ See *The EU Dual Use Export Control Regime*, European Commission, at 2 (Feb. 2, 2014), http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152181.pdf.



Canada, New Zealand, Japan, Norway, Switzerland, and the United States — are only slightly more encumbered: any EU Member State exporter may use EU General Export Authorization number 001(EU GEA 001) to send Annex I goods to one of the friendly countries, by simply notifying the Member State from which they are exporting within 30 days after their first export.¹⁰ EU Member States may require exporters to register prior to using EU GEA 001, but such registration “shall be automatic and acknowledged by the competent authorities to the exporter without delay and in any case within ten working days of receipt.”¹¹ For most (if not all) of the Member States, this additional requirement is a simple, one-time pre-registration process.¹² Under the Proposed Rule, meanwhile, U.S. exporters will plead for their would-be students and customers’ patience as they await issuance of BIS licenses — unless, of course, the needed instruction, products, and technology confront a presumption of denial that could effectively bar export altogether.

In sum, the Proposed Rule will be damaging for Offensive Security and for the U.S. cybersecurity industry by creating an uneven international playing field.

¹⁰ *See id.* at 254.

¹¹ *See id.*

¹² *See, e.g., Open General Licences: An Overview*, UK Export Control Organisation (Aug. 23, 2012), <https://www.gov.uk/open-general-licences-an-overview>; *Brief Outline on Export Controls*, The Federal Office of Economics and Export Control, at 11 (2013), http://www.bafa.de/bafa/en/export_control/publications/export_control_brief_outline.pdf; *User Guide on Strategic Goods and Services for The Netherlands*, Ministry of Foreign Affairs, at 30 (2013), available at <http://www.government.nl/issues/export-controls-of-strategic-goods/documents-and-publications/directives/2012/04/12/user-guide-on-strategic-goods-and-services.html>.



B. The Proposed Rule Would Undermine the Prevention of Cybersecurity Attacks Worldwide

The Proposed Rule will also hinder the defensive cybersecurity efforts of U.S. and non-U.S. entities with foreign locations. Perhaps most problematic is that the Proposed Rule eliminates the license exception for exports to subsidiaries of U.S. corporations, or to employees or contractors of U.S. firms at 15 C.F.R. § 740.17 that has served long and well the core of U.S. companies that make and export encryption functionality software and technology.

And because the need for defensive security software and technology often arises immediately (*e.g.*, in an emergency breach situation), when delay occasioned by a license application requirement can be fatal to a cyberdefense objective, the Proposed Rule will render non-U.S. entities — including the many foreign subsidiaries of U.S. companies that Offensive Security counts among its customer base — more susceptible to damage from cyberattacks. Indeed, the Proposed Rule may diminish even the security of U.S. companies at home as oftentimes a vulnerability at a foreign subsidiary can provide an attack vector into domestic networks and systems.

Although U.S. subsidiaries might more easily source instructional materials and penetration-testing products and technology from abroad, these materials may not be as effective as those provided by U.S. firms, and U.S. subsidiaries may lack the familiarity and experience with foreign-sourced products that they would have with U.S.-origin products and services.

The unavailability of a license exception for deemed exports of controlled software and technology to employees or contractors of U.S. firms would also add an administrative burden and additional layer of diligence to the process of providing software and technology to even household-named U.S. firms.



These anticipated casualties of the Proposed Rule seem far too high a price to pay for discharging U.S. commitments under the Wassenaar Arrangement, and especially in light of how other member countries are satisfying their equivalent commitments.

C. The Proposed Rule Would Be Ineffective to Thwart Malicious Actors

Offensive Security believes that the Proposed Rules would be largely ineffective to achieve their desired aim. The damaging effects of the Proposed Rule are abundant, yet its benefits are difficult to perceive. To begin, the Proposed Rule does not address the delivery of offensive exploits utilizing entirely domestic tools. And the Proposed Rule does not control or even address the vast majority of situations involving the delivery of harmful software, malware, and spyware. In most cases of malicious intent, Offensive Security believes that an actor will develop a harmful exploit, test the harmful exploit, deliver the harmful exploit, and then maliciously attack a network or system without in any way utilizing software or technology affected by the Proposed Rule. As one such example, assume that a malicious actor creates an exploit based on an SQL injection (*i.e.*, malicious SQL statements inserted into an entry point for execution). The exploit itself, a string of SQL code, will not be controlled by the Proposed Rule because the Proposed Rule does not control exploits. Now assume the malicious actor delivers the SQL injection to the target using standard HTTP. Because HTTP (and the components required to invoke HTTP) is not specially designed or modified for the “generation, operation or delivery of, or communication with, intrusion software,” it would not be controlled by the Proposed Rule. Additionally, assume that the command and control used to read and write to the network connection is Netcat, a common and publicly available open-source tool. Here again, because Netcat is open-source and freely and publicly available, it also would not be controlled by the Proposed Rule. Even if the SQL injection represented a zero-day exploit, nothing described in the above scenario would appear to trigger the restrictions in the Proposed Rule.



To take an example that is real and current, the internal corporate records of Italian-based Hacking Team were compromised and over 400GB of its data were leaked to the Internet.¹³ This exposed the Hacking Team as a provider of its intrusion-delivery platform — capable of serious misuse in the hands of governments conducting surveillance on their citizens — to governments involved in mass genocide such as in Sudan. *Id.* At this point it remains unclear whether the Italian-based Hacking Team and the apparent provision of software and services to Sudan were even subject to U.S. jurisdiction, so it remains unclear whether the Proposed Rule would have had *any* affect over Hacking Team’s unscrupulous provision of assistance to the Sudanese government. But even if those activities were subject to U.S. jurisdiction, the supply of software to the Sudanese government was already unlawful under the EAR and U.S. economic sanctions against Sudan. To suggest that the addition of the restrictions in the Proposed Rule would prevent these sorts of occurrences simply rings hollow, yet the cost of adding the restrictions is undeniable.

Indeed, most malicious cyberattacks will not be affected at all by the Proposed Rule — and particularly because tools widely used for generating, delivering, or controlling exploits are open-source and freely available, or else not otherwise subject to U.S. jurisdiction, and so could not be affected by the Proposed Rule. *See* 15 C.F.R. § 734.3(b)(3). Malicious actors are not likely to engage Offensive Security for its training and consulting services, as Offensive Security notifies third-party software vendors or otherwise publishes its discovered exploits when developing custom tests for a customer’s environment. Importantly, Offensive Security’s training and services have been used for legitimate defensive purposes hundreds of thousands of times.

¹³ Valentino-Devries, Jennifer and Yadron, Danny, “Hacking Team, the Surveillance Tech Firm, Gets Hacked,” *The Wall Street Journal* (Jul. 6, 2015) (available at <http://www.wsj.com/articles/hacking-software-maker-gets-hacked-1436223757>).



III. Proposed Modifications to the Proposed Rule

A fundamental problem with the Proposed Rule is that it too restrictively controls a broadly defined category of intrusion-delivery training materials, software, and technology that is fundamental to protecting global networks and systems. In an effort to pare back the Proposed Rule's broad, counterproductive effects, we offer the following suggestions.

A. Current Export Controls And License Exceptions Are Adequate

As a first suggestion, we would ask BIS to reconsider implementing the Wassenaar Arrangement under the existing provisions of License Exception ENC.

Offensive Security believes that the current regime adequately and effectively balances the global need to secure networks and systems with the compelling interest of making it difficult for malicious software to be obtained by malicious actors or used maliciously. Some of the most important, widely used license exceptions available for the export of software and technology authorize exports to U.S. subsidiaries abroad, private sector end-users wherever located that are headquartered in a country listed in Supplement No. 3 to Part 740 of the EAR, businesses located abroad but headquartered in the United States, and foreign developers and contractors of a U.S. company, as specified in 15 C.F.R. § 740.17(a). Offensive Security believes that it would benefit greatly if these license exceptions were also made available for intrusion-delivery software and technology.

It is hard to understand the rationale for a wholesale elimination of these types of license exceptions in the Proposed Rule, since the encryption regulations have long operated on precisely this basis, without apparent detriment to the national security and with a diminished regulatory burden on BIS. Indeed, hundreds of legitimate private- and public-sector businesses rely on Offensive Security's training, consulting services, and technology, yet many of Offensive



Security’s students and customers, and/or their foreign branches and subsidiaries, would be suddenly denied protection under the Proposed Rule.

And the unavailability of the important license exceptions for deemed exports of controlled software and technology to employees or contractors of U.S. corporations would unnecessarily retard the advancement of security technology and research and development for U.S. corporations. We predict and fear a drain of technical talent as a result of the Proposed Rule.

B. License Exception for Educational and Training Materials

As explained above, an important facet of Offensive Security’s business is the provision of training courses and technical certifications to students (and professionals) seeking education and ultimately employment in the security industry.

Offensive Security thus recommends that the Proposed Rules should contemplate broad license exceptions that permit it to provide all of its training courses, materials, and related technology and software without applying for individual end-user licenses for each non-U.S. student wishing to take a course offered by Offensive Security. This type of exception would be important to Offensive Security because it is not able to make its training courses entirely freely and publicly available — this is how Offensive Security earns revenues to support its business and community projects.

As part of a license exception for educational and training materials, BIS could require the provider of educational instruction to obtain written end-use statements thereby committing end-users to educational, training, and defensive uses of the software and technology on networks, software, systems, and hardware, owned and controlled by the instructor or the student. And BIS could enforce significant civil and criminal penalties against an end-user for violation of this end-use statement. This would bring the regulation of intrusion software in line



with other laws and regulations (*e.g.*, Computer Fraud and Abuse Act and the Electronic Communications Privacy Act) whose proscriptions turn on specific conduct and intent rather than the technical characteristics of an item on which scores of legitimate companies and government entities rely to protect their networks.

C. Clarification of Controlled Technology

Offensive Security believes that the Proposed Rule fails to help the regulated public identify what “technology” would be controlled. Without a clear articulation of these important concepts, the level of actual compliance with the rule that is finally implemented is almost certain to be low.

As explained above, an important part of Offensive Security’s business is providing consultation services and security assessments to its customers, often including information on how to conduct customer-specific penetration testing to protect the customers’ networks and systems. Arguably, the consultation services, security assessments, and related information flowing to and from the customer constitute technical information meeting the definition of controlled technology pursuant to the Proposed Rule, leaving Offensive Security without clear guidance for how to deal with its non-U.S. customer base. Offensive Security believes that the ambiguity in the definitions and control of “technology” would create an unworkable regulatory regime.

D. License Exceptions for Exports to the EU and Friendly Countries

The effectiveness of a multi-lateral export control regime such as the Wassenaar Arrangement depends not only on the signatories agreeing to specific language defining the technical categories of items on the Commerce Control List, but also and more importantly on similar licensing and control practices amongst the signatories. As explained, however, the EU has *not* implemented Draconian controls such as those outlined in the Proposed Rules has instead



authorized the free flow of intrusion software among and between EU countries, and even to countries outside of the EU, including the United States. BIS should at a minimum implement license exceptions authorizing export to friendly countries such as the EU Member States and other Wassenaar signatories. Absent such parity of treatment, it is hard to see why any company in this space would remain in the United States, where the proposed barriers to export and research/development work are so high.

IV. Offensive Security’s Responses to Questions Posed By the Proposed Rule

- 1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:**

Offensive Security estimates that it could be required to submit hundreds of license applications per year under the requirements of the proposed rule.

- a. How many additional applications would be for products that are currently eligible for license exceptions?**

Because of the ambiguities created by the Proposed Rule regarding the provision of controlled technology, it is difficult for Offensive Security to estimate precisely how many additional license applications would be required for exports of controlled technology to students and customers. Potentially, the Proposed Rule would require Offensive Security to submit hundreds of license applications per year for items that are currently eligible for license exceptions.



b. How many additional applications would be for products that currently are classified EAR99?

Offensive Security does not believe that it would be required to submit any additional license applications under the Proposed Rule for products that are classified as EAR99.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

Offensive Security estimates that it would be required to submit dozens of deemed export license applications per year under the requirements of the Proposed Rule. These license applications may include applications for Offensive Security's non-U.S. employees and instructors, as well as for the provision of controlled technology to Offensive Security's U.S. customers who employ non-U.S. citizens.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

Yes, for all of the reasons provided above, the Proposed Rule would have negative effects on Offensive Security's legitimate vulnerability research, audits, testing and screening, as well as Offensive Security's ability to protect its own and its clients networks.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? If this information you already have for your products?

Offensive Security estimates that it would take approximately forty (40) hours to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748. In the ordinary course



of its business, Offensive Security does not maintain the information organized in the manner requested by the supplement.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k37-706c
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0141

Comment on FR Doc # 2015-11642

Submitter Information

Name: Raphael Mudge

Address:

1875 Connecticut Ave NW

10th Floor

Washington, DC, 20009

Email: raffi@strategiccyber.com

Phone: 8887617773

General Comment

See attached file.

Attachments

stratcyber_comment_RIN_0694-AG49



20 July 2015

FROM: Raphael S. Mudge
Principal, Strategic Cyber LLC
1875 Connecticut Ave NW
10th Floor
Washington, DC 20009

SUBJECT: Public Comment for RIN 0694-AG49 / BIS-2015-0011
Proposed Rule titled "*Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items*"

Strategic Cyber LLC is the manufacturer of Cobalt Strike, a network penetration testing product. This product is sold for lawful and ethical penetration testing purposes. Strategic Cyber's customers are organizations who must assess their intrusion detection and response processes against the same tactics sophisticated adversaries use. This use case requires software and a controller that exfiltrates data and evades defenses in a way that meets the definition of ECCN 4D004 in the Proposed Rule. This Public Comment focuses on the impacts of the Proposed Rule to Strategic Cyber LLC and the consumers of Cobalt Strike.

Strategic Cyber LLC understands that the purpose of the Proposed Rule is to meet the U.S.'s obligations under the Wassenaar Arrangement (WA) to control the export of cybersecurity technologies. WA doesn't determine how the United States implements the new controls. It only requires that the U.S. and other WA Participating States control the export of cybersecurity software and hardware and technology from their respective jurisdictions. The WA moved to control these technologies to prevent the acquisition of cybersecurity technologies by oppressive regimes.

Today, Cobalt Strike and other penetration testing software products that use encryption are classified under ECCN 5D002. Strategic Cyber LLC exports its products through the use of License Exception ENC provisions in Part 740.17 of the Export Administration Regulations (EAR). These provisions impose due diligence screening and reporting requirements that Strategic Cyber LLC follows. Strategic Cyber LLC may export its software without a validated license to a list of countries in Supplement No. 3 to Part 740 of the EAR. This list of countries, primarily EU countries plus Australia, Canada, New Zealand and Japan, does not include oppressive regimes.

Strategic Cyber LLC is concerned that the Proposed Rule goes far beyond the United States' obligation to the WA and beyond the controls implemented by other WA countries. The proposed U.S. implementation would create an uneven playing field by placing U.S. companies like Strategic Cyber at a competitive disadvantage with companies from other WA Participating States.

Strategic Cyber LLC asks that BIS modify the Proposed Rule to allow export rights and exceptions similar to what the encryption controls specify for penetration testing software today.

The current approach meets the U.S.'s obligations under the WA and these rules, already in effect for most commercial penetration testing software, would minimize the impact of the new controls on the U.S. cybersecurity industry.

The new proposed licensing requirements will have a substantial impact on Strategic Cyber LLC's ability to make sales to commercial and government entities within countries that are close allies to the United States (to include FVEY and NATO countries). Strategic Cyber LLC's price model was designed to keep the product accessible to individual consultants. This price model cannot support the administrative burden to request export licenses for each evaluation request of the Cobalt Strike product, when only a handful of evaluations convert to sales. If the Proposed Rule is enacted with the license requirement for each export intact, Strategic Cyber LLC may be forced to opt against participation in foreign markets. Again, this provides opportunity for a foreign competitor to thrive at the expense of a U.S.-based business.

BIS has stated that it anticipates broad license authorizations to certain types of end-users and destinations to counterbalance the loss of the ENC License Exceptions. Strategic Cyber LLC prefers ENC's exceptions over this solution. If broad authorizations are the compromise, then Strategic Cyber LLC asks that BIS modify the Proposed Rule to document these broad end-user and destination license authorizations. The Proposed Rule should document which combination of end-user and destination authorizations a company may apply for and the criteria to receive it. If this issue is "left for later" it will create an unpredictable climate for foreign businesses to buy penetration testing software from U.S.-based businesses.

Strategic Cyber LLC asks that BIS modify the Proposed Rule to allow for License Exception TSU to distribute software updates and maintenance technology to customers who receive a lawfully exported 4D004 product.

The Proposed Rule does not provide a license exception for software updates and maintenance technology related to 4D004 products. Strategic Cyber LLC releases updates to its product four to six times per year. Regular updates to keep up with customer needs are an expectation from consumers of penetration testing products. It's not tractable for Strategic Cyber LLC to request an export license for each of its foreign customers for each update of its software.

Strategic Cyber asks that BIS introduce a license exception for intra-company transfers of intrusion and surveillance items.

As written, the Proposed Rule creates great pain for multinational companies with headquarters in the United States. These companies buy software from U.S.-based businesses for use at foreign and domestic offices. The users at these offices are sometimes foreign nationals. The Proposed Rule does not provide an exception for intra-company transfers. This omission would require a multinational company headquartered in the United States to request an export license to use the software they bought from a U.S. vendor at their foreign sites or by their foreign employees. Key members of some U.S. headquartered multinational company security are teams located outside of the United States. This could lead to situations where these U.S.-based companies may choose to buy a foreign vendor's product due to the lack of restrictions on its use at all of their sites, by any of their employees.

Strategic Cyber asks that BIS introduce a license exception for tools of the trade for intrusion and surveillance items.

The United States enjoys the benefits of a healthy cybersecurity industry with consultants whose services are in-demand, all over the world. U.S.-based consultants are often hired to travel to a foreign site and provide a security assessment of that site. Some types of security assessments are conducted remotely, but most penetration tests take place with the consultant team at or near the customer's site. The Proposed Rule does not include a tool of the trade exception that allows U.S. nationals to carry their tools to a customer site in a foreign country. It's critical that U.S. nationals have the right to use their tools, bought from a U.S. vendor, at all customer sites. If commercial penetration testing products of U.S. origin are difficult to use because of regulation, U.S. nationals may shy away from these products and use a public domain product or buy from a foreign competitor. This hurts the quality of service a U.S. national can provide to foreign customer sites and it hurts the U.S.'s penetration testing software vendors.

Strategic Cyber asks that BIS modify the Proposed Rule to remove the presumption of denial for zero-day exploits.

Penetration Testing products are regularly updated with the latest offensive technology. This activity is necessary to help customers stay ahead of adversaries by allowing them to evaluate their networks against the latest attack techniques, as quickly as possible. The Proposed Rule describes a presumption of denial for zero-day exploits and rootkit technologies. Strategic Cyber LLC is concerned about this presumption of denial and the lack of a legal definition, vetted by subject matter experts, for these terms. If either of these terms is poorly defined, BIS may inadvertently make U.S.-based commercial penetration testing products un-exportable depending on what future updates may contain.

This issue shows itself with the lack of a definition for zero-day exploit. If BIS defines a zero-day exploit as an exploit for a vulnerability without a publicly available patch, then the Proposed Rule will prevent the export of penetration testing products from U.S. companies when a new attack is discovered and integrated into a commercial penetration testing platform. This quick integration is necessary to allow customers an immediate way to test their systems AND defenses against the new attack technique.

Strategic Cyber asks that BIS modify the Proposed Rule to remove the presumption of denial for rootkit technologies.

Strategic Cyber defines a rootkit as a post-exploitation technology that installs itself below or into the operating system's kernel to hide an attacker's actions. Today, rootkits are not a common demand from consumers of penetration testing products. If a novel new method of installing a rootkit is discovered, it's likely that consumers of penetration testing products will ask for a rootkit technology from their vendors. A presumption of denial on this technology is a forward-looking statement from BIS about which technologies organizations will need to exercise their detection and response mechanisms against a representative adversary. Rootkit technologies are another method to avoid detection and they are already covered under the definition of Intrusion Software.

Strategic Cyber asks that BIS consider these comments and issue another Proposed Rule with its modifications; followed by another period of public comment.

This approach will give the U.S. security industry an opportunity to advise BIS on the proposed changes and help find a policy solution that is in harmony with policy goals and lawful commerce.

Strategic Cyber LLC is also happy to offer its assistance and answer questions related to the rewrite of the Proposed Rule. If I may be of service, my contact information is below.

//signed

RAPHAEL S. MUDGE
Principal, Strategic Cyber LLC

e-mail: raffi@strategiccyber.com
phone: 1-888-761-7773
twitter: @armitagehacker
www: <http://www.advancedpentest.com/>

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k38-jp7a
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0142

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Osborn

Address:

Goodwin Procter LLP
901 New York Avenue NW
Washington, DC, 20001

Email: josborn@goodwinprocter.com

Phone: 202-346-4133

Fax: 202-346-4444

Organization: Pwnie Express

General Comment

See attached file(s)

Attachments

Pwnie Express's Comments to BIS's Proposed Rule - FINAL



Pwnie Express’s Comments to “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items,” 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63.

Rapid Focus Security, Inc. (d/b/a and hereinafter “Pwnie Express”), a Delaware corporation that develops and sells professional penetration-testing hardware devices, submits these comments to the rule proposed by the Bureau of Industry and Security (“BIS”) involving the control of intrusion-delivery hardware and software. *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63 (“Proposed Rule”). Pwnie Express believes the Proposed Rule would have consequences that are unintended and extremely detrimental to the U.S. penetration testing industry and ultimately to the U.S. national security.

In Part I below, Pwnie Express introduces its business and the products relied upon by its customers for network and system security. In Part II, Pwnie Express explains why it believes the Proposed Rule would: (i) damage Pwnie Express’s business and other U.S. businesses operating in the security space; (ii) have a detrimental effect on cybersecurity and preventing cyberattacks worldwide; and (iii) be ineffective as a means to thwart malicious actors — including human-rights abuses abroad — who use intrusion software for offensive and malicious purposes. In Part III, Pwnie Express recommends modifications to the Proposed Rule that would alleviate the concerns expressed in Part II. And, in Part IV, Pwnie Express provides responses to the specific questions posed by BIS. *See* Proposed Rule at 28856.

I. Pwnie Express’s Business and Offerings

Founded in Vermont in 2010, Pwnie Express is a manufacturer of security hardware products that ship with pre-installed software. Pwnie Express’s hardware products, called “sensors,” are made available in various off-the-shelf form factors, such as smartphones and tablets. These sensors permit IT professionals to conduct penetration testing to evaluate the security of wired, wireless, and Bluetooth networks.



The Pwnie Express software stack installed on the sensors is the same across all Pwnie Express hardware products with respect to the cryptographic, penetration-testing, and cryptanalytic capabilities. Pwnie Express does not develop intrusion or testing software, but simply packages together many open-source, publicly available testing components into a single, easy-to-use software image, and then pre-installs this image on off-the-shelf mobile devices. Pwnie Express has previously provided BIS with a complete list of the open-source third-party components that comprise its software stack as part of a Classification Request. Pwnie Express also has a history of working cooperatively with BIS to ensure its compliance with the EAR.

II. Negative Impact of The Proposed Rule

The United States government, public, and business community have a shared interest in ensuring that malicious software is not obtained by malicious actors or used maliciously — indeed, never has the need for protection against cyber intrusions been more acute than it is today. But this is precisely why it is vital to maintain and encourage U.S. dominance in this space, and to ensure that *defensive* products, services, and technology, such as those offered by Pwnie Express, are available for use in protecting enterprises, government, and individuals. The Proposed Rule threatens to damage Pwnie Express’s business and this industry in the United States, driving it offshore and, ultimately, outside of the reach of U.S. jurisdiction and regulation.

A. The Proposed Rule Would Damage Pwnie Express and Other U.S. Businesses

Pwnie Express’s hardware offerings with pre-installed intrusion-delivery software would appear to meet the criteria of 4A005 as equipment that is modified for the generation, operation or delivery of, or communication with, intrusion software. As explained by the Proposed Rule, Regional Stability (“RS”) controls would apply to intrusion-delivery hardware and would require a validated license for export to all foreign countries other than Canada. The Proposed Rule would thus eliminate Pwnie Express’s eligibility for License Exception ENC — indeed, other than a limited GOV license exception for exports to the U.S. government, there would be no license exception available for these products.



The Proposed Rule threatens to drastically increase the administrative burden for the roughly 30% of Pwnie Express’s sales that are made outside of the United States. This is a particularly vexing problem for Pwnie Express, given that the high volume yet low price point (ranging from \$995 to \$1,995 per unit) and profit margin of Pwnie Express’s products may not justify the compliance and administrative burdens involved in applying for, and obtaining licenses for all exports of its products. This includes sales to the foreign branch offices and foreign subsidiaries of iconic U.S. companies, to allies of the United States, and to multinational companies whose networks house data belonging to U.S. companies or the protection of which is otherwise vital to the U.S. national security. It is perplexing that, in the name of denying offensive tools to bad actors intent on doing harm to the United States, the Proposed Rule would remove from these and many other legitimate organizations the critical tools necessary to defend themselves against cyberattacks.

The Proposed Rule would also severely limit Pwnie Express’s ability to employ or engage non-U.S. citizens, since it would require that Pwnie Express apply for “deemed export” licenses. We expect that the U.S. domestic development of defensive cybersecurity tools will decline as foreign talent for this critical work will become harder or impossible to attract and manage. Given the ambiguous contours separating controlled technology from non-controlled technology (even under the most clearly worded regulations in the EAR), it may be impractical and perhaps impossible to restrict non-U.S. workforce to exclusively non-controlled software and technology, leaving as the only alternative an exclusively U.S. workforce. This will tend to diminish the effectiveness of cybersecurity products made in the United States.

Many other U.S. businesses are likely to be similarly affected and placed at a competitive disadvantage vis-à-vis foreign-based security firms providing hardware and technology of non-U.S. origin. The administrative burdens created by the licensing process and necessary for sales to foreign customers would be detrimental to U.S. industry. Significant time, costs, and legal fees would be required to understand and comply with the license application process for each foreign customer and employee. Also significant would be the delay between when a



penetration-testing product is needed and when a BIS license would issue to authorize its exportation.

Another obvious consequence of the Proposed Rule is to confer on non-U.S. producers of intrusion-delivery hardware and technology a insuperable advantage over U.S. firms. Although each signatory to the Wassenaar Arrangement has committed to controlling intrusion-delivery items, none appears to have adopted anything approaching the extent of restriction set forth in the Proposed Rule. For instance, the European Union has implemented minimal controls to intrusion-delivery items by adding the item to Annex I to Regulation (EC) No. 428/2009.¹ Except for a subset of Annex I items designated for stricter controls and listed in Annex IV, the transfer of items within the EU community only requires exporters to maintain records for at least three years, and indicate on the commercial documents that accompany the items that they are subject to further controls if exported from the EU community.² The vast majority of Annex I items, including intrusion-delivery items, may be traded freely — without registration or licensing — within the EU community.³ Exports from EU Member States to seven “friendly countries” — Australia, Canada, New Zealand, Japan, Norway, Switzerland, and the United States — are only slightly more encumbered: any EU Member State exporter may use EU General Export Authorization number 001(EU GEA 001) to send Annex I goods to one of the friendly countries, by simply notifying the Member State from which they are exporting within 30 days after their first export.⁴ EU Member States may require exporters to register prior to using EU GEA 001, but such registration “shall be automatic and acknowledged by the

¹ See Commission Delegated Regulation 1382/2014, at 13, 130-31, http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf.

² See Council Regulation 428/2009, Annex IV, pp.260-66, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF>. Annex IV includes military, cryptologic, and chemical-weapons related items that are subject to additional restrictions, even when transferred within the EU community. See also Council Regulation 428/2009, Ch. VIII, art. 22(1), p.9; Ch. VIII, art. 22(8) p.10; Ch. VIII art. 22(10), p.10.

³ See *The EU Dual Use Export Control Regime*, European Commission, at 2 (Feb. 2, 2014), http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152181.pdf.

⁴ See *id.* at 254.



competent authorities to the exporter without delay and in any case within ten working days of receipt.”⁵ For most (if not all) of the Member States, this additional requirement is a simple, one-time pre-registration process.⁶

In sum, the Proposed Rule will be damaging for Pwnie Express and for the U.S. cybersecurity industry by creating an uneven international playing field.

B. The Proposed Rule Would Undermine the Prevention of Cybersecurity Attacks Worldwide

The Proposed Rule will hinder the defensive cybersecurity efforts of U.S. and non-U.S. entities with foreign locations. Perhaps most problematic is that the Proposed Rule eliminates the EAR License Exception ENC as it relates to exports to subsidiaries of U.S. corporations, or to employees or contractors of U.S. firms — exceptions of the sort found at 15 C.F.R. § 740.17 that have served long and well the hundreds of U.S. companies that make and export encryption functionality software.

And because the need for defensive security hardware and technology often arises immediately (*e.g.*, in an emergency breach situation), when delay occasioned by a license application requirement can be fatal to a cyberdefense objective, the Proposed Rule will render non-U.S. entities more susceptible to damage from cyberattacks.

Although U.S. subsidiaries might more easily source penetration-testing products from abroad, these products may not be as effective as those provided by U.S. firms, nor might U.S.

⁵ *See id.*

⁶ *See, e.g., Open General Licences: An Overview*, UK Export Control Organisation (Aug. 23, 2012), <https://www.gov.uk/open-general-licences-an-overview>; *Brief Outline on Export Controls*, The Federal Office of Economics and Export Control, at 11 (2013), http://www.bafa.de/bafa/en/export_control/publications/export_control_brief_outline.pdf; *User Guide on Strategic Goods and Services for The Netherlands*, Ministry of Foreign Affairs, at 30 (2013), available at <http://www.government.nl/issues/export-controls-of-strategic-goods/documents-and-publications/directives/2012/04/12/user-guide-on-strategic-goods-and-services.html>.



subsidiaries have the familiarity and experience with foreign-sourced products as they would have with U.S.-origin products and services.

The unavailability of a license exception for deemed exports of controlled software and technology to employees or contractors of U.S. firms would also add an administrative burden and additional layer of diligence to the process of providing software and technology to even household-named U.S. firms.

These infirmities in the Proposed Rule seem far too high a price to pay for discharging U.S. commitments under the Wassenaar Arrangement, and especially given that other member countries are satisfying their equivalent commitments with restrictions far lesser in scope and effect than the Proposed Rule.

C. The Proposed Rule Would Be Ineffective to Thwart Malicious Actors

The damaging effects of the Proposed Rule are abundant, yet its promised benefits are difficult to understand. The Proposed Rule does not control or even address the vast majority of situations involving the delivery of harmful software, malware, and spyware. In most cases of malicious intent, Pwnie Express believes that an actor will develop a harmful exploit, test the harmful exploit, deliver the harmful exploit, and then maliciously attack a network or system without in any way utilizing hardware or technology affected by the Proposed Rule.

Pwnie Express believes that most malicious cyberattacks will not be affected at all by the Proposed Rule —particularly because many of the tools widely used for generating, delivering, or controlling exploits are open-source and freely available, or else not otherwise subject to U.S. jurisdiction, and could not be affected by the Proposed Rule. *See* 15 C.F.R. § 734.3(b)(3). These open-source, freely available tools are far more likely to be called upon by actors intent on perpetrating malicious cyberattacks than are the legitimate, professional penetration-testing products offered by Pwnie Express and its competitors.



III. Proposed Modifications to the Proposed Rule

A fundamental problem with the Proposed Rule is that it too restrictively controls a broadly defined category of intrusion-delivery hardware, software, and technology that is fundamental to protecting global networks and systems. In an effort to pare back the Proposed Rule’s broad, counterproductive effects, we offer the following suggestions.

A. Current Export Controls Are Adequate

As a first suggestion, we would ask BIS to consider implementing the Wassenaar Arrangement under the existing provisions of License Exception ENC, which are likely to apply to most or possibly all affected forms of intrusion software.

Based on experience working under the encryption-controls regulations, we think the current regime adequately and effectively balances the global need to secure networks and systems and the compelling interest of making it difficult for malicious hardware and software to be obtained by malicious actors or used maliciously. Under the current regime, Pwnie Express provides detailed, product-specific Classification Requests to BIS. Pwnie Express is also required to provide BIS with semi-annual reports detailing all exports of its sensors. And for foreign government end-users, Pwnie Express is required to obtain a license before exporting its products. These controls are adequate.

B. Control Only Those Tools With No Legitimate Defensive Uses

If BIS is determined to remove the eligibility of License Exception ENC for intrusion-delivery software, then the rule should be made to apply to those tools for which there are no apparent, legitimate defensive uses. For instance, the FinFisher software and the Zeus Zbot are software products that are overtly offensive and malicious. The Hacking Team platform that was targeted to government end-users is another example. Products that include non-consensual tracking and monitoring technology (*i.e.*, designed to allow a mobile or networked device to reveal its geographic location and operating status or application data without consent of the device owner or content provider), or censorship-enhancing technology (*i.e.*, designed to enforce



content blocking or fingerprinting and defeating anticensorship technologies) are also examples of products that may have no legitimate, defensive use. These are the types of products that should be the focus of BIS's efforts.

Just as the Proposed Rule has brought together competitors and collaborators to discuss how best to discharge the United States's Wassenaar Arrangement obligations, we think it would be a grave and costly mistake to conclude, without substantial effort, that BIS, working hand-in-hand with the affected industry members, could not draft a rule that distinguishes offensive products from legitimate, defensive cybersecurity solutions of the sort that Pwnie Express provides to customers worldwide. For instance, BIS is already able to review the materials submitted in support of a Classification Request to determine whether the products under review have legitimate defensive purposes. BIS could further require an exporter to provide details about why and how a given item has legitimate defensive purposes, a predominantly defensive intention, and why the product is not well suited for offensive uses. In that way, malware-delivery, spyware-delivery, and malicious exploits-delivery products having only offensive purposes could be appropriately restricted in their distribution, leaving legitimate, defensive products free of restrictions that could frustrate its foreign distribution altogether.

BIS could also rely more substantially on written end-use statements committing end-users to defensive uses of the products on their owned and controlled networks and systems, and committing such end-users to audits or visits by BIS agents to test compliance. And BIS could enforce significant civil and criminal penalties against an end-user for violation of this end-use statement. This would bring the regulation of intrusion hardware in line with other laws and regulations (*e.g.*, Computer Fraud and Abuse Act and the Electronic Communications Privacy Act) whose proscriptions turn on specific conduct and intent rather than controlling items based on purely technical characteristics.

C. License Exceptions for Exports to U.S. Subsidiaries, Developers, and Contractors for Internal Company Use

A few of the most important license exceptions available for the export of encryption items are those to U.S. subsidiaries, businesses headquartered in the United States, and foreign



developers and contractors of a U.S. company, as specified in 15 C.F.R. § 740.17(a). It is hard to understand that rationale for eliminating these types of license exceptions in the Proposed Rule, since the encryption regulations have long operated on precisely this basis, and without apparent detriment to the national security.

As explained above, the unavailability of license exceptions for exports to U.S. subsidiaries and businesses headquartered in the United States would have a profound detrimental effect on preventing cyberattacks worldwide. Corporations have a compelling need to respond immediately to an attack, taking any and all defensive measures possible. This is not possible without self-effectuating license exceptions of the sort available in 15 C.F.R. § 740.17(a).

And the unavailability of the important license exceptions for deemed exports of controlled software and technology to employees or contractors of U.S. corporations would unnecessarily retard the advancement of security technology and research and development for U.S. corporations. We fear a drain of technical talent as a result of the Proposed Rule.

D. License Exceptions for Exports to the EU and Friendly Countries

The effectiveness of a multi-lateral export control regime such as the Wassenaar Arrangement depends not only on the signatories agreeing to specific language defining the technical categories of items on the Commerce Control List, but also on similar licensing and control practices amongst the signatories. As explained, however, the EU has *not* implemented Draconian controls such as those outlined in the Proposed Rules and instead is content with a control regime that authorizes free flow of intrusion-delivery items among and between EU countries, and even outside of the EU. BIS should at a minimum implement license exceptions authorizing export to friendly countries such as the EU Member States and other Wassenaar signatories. Absent such parity of treatment, it is hard to see why any company in this space would remain in the United States, where the Proposed Rule would erect such high barriers to export.



E. Clarification of Controlled Technology

Pwnie Express believes that the Proposed Rule fails to help the regulated public identify what “technology” would be controlled. Yet without a clear articulation of these important concepts, the level of actual compliance with the rule that is finally implemented is almost certain to be low.

On occasion Pwnie Express’s business involves customer support for its products — *i.e.*, training and information on how to use the Pwnie Express products in order to conduct penetration testing to protect the customers’ networks and systems. Would training on how to use this functionality be considered controlled technology regarding the “development or production of the command delivery platform itself,” or “information on how to prepare the exploit for delivery or integrate it into a command and delivery platform”?⁷ Or, would it instead be considered decontrolled “information ‘required for’ developing, testing, refining, and evaluating ‘intrusion software’”?⁸ Arguably, this type of technical training meets both criteria, leaving Pwnie Express without clear guidance for how to deal with its non-U.S. customer base.

Pwnie Express believes that the ambiguity in the definitions and control of “technology” would create an unworkable regulatory regime.

IV. Pwnie Express’s Responses to Questions Posed By the Proposed Rule

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

Pwnie estimates that it would be required to submit approximately 200 total license applications per year under the requirements of the proposed rule.

⁷ See BIS FAQ #4, available at <http://www.bis.doc.gov/index.php/policy-guidance/faqs>.

⁸ *Id.*



a. How many additional applications would be for products that are currently eligible for license exceptions?

Pwnie Express estimates that it would be required to submit approximately 200 license applications per year under the Proposed Rule for products that are currently eligible for license exceptions.

b. How many additional applications would be for products that currently are classified EAR99?

Pwnie Express does not believe that it would be required to submit any additional license applications under the Proposed Rule for products that are classified as EAR99.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

Pwnie Express does not believe that it would be required to submit any deemed export license applications per year under the requirements of the Proposed Rule.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

Yes, for all of the reasons provided above, the Proposed Rule would have negative effects on Pwnie Express's ability to protect its clients networks.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? If this information you already have for your products?

Pwnie Express estimates that it would take approximately forty (40) hours to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748. In the ordinary course of its business, Pwnie Express does not maintain the information organized in the manner requested by the supplement.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k38-nx27
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0143

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael Beckerman

Address:

The Internet Association
1333 H Street NW
Washington, DC, 20002

Email: slater@internetassociation.org

Phone: (202) 770-0023

General Comment

See attached file(s)

Attachments

FINAL Comments on BIS Implementation of Wassenaar on LH-2



INTERNET ASSOCIATION COMMENTS ON BIS IMPLEMENTATION OF THE WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS ON INTRUSION AND SURVEILLANCE ITEMS

1. Introduction

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies and their global community of users.¹ It is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Network security is of paramount importance to our member companies. They work tirelessly to defend their networks and their users' data from unlawful intrusions. Public policies that undermine the ability of security researchers to protect networks – whether by design or by default – are therefore highly relevant and important to us.

The members of the Internet Association would like to thank the Bureau of Industry and Security (BIS) for providing an open comment period regarding proposed changes to the Export Administration Regulations (EAR) implementing the Wassenaar Arrangement 2013 Plenary Agreements Implementation on Intrusion and Surveillance Items. We applaud BIS officials for requesting input to better understand how companies approach security and how this rule may negatively impact those capabilities.

Implementation of the Wassenaar Arrangement in the intrusion software space is an important topic with a number of complex and potentially competing interests. The recent compromise at Hacking Team in Italy puts this complexity in stark focus. While Italy had implemented the provisions of the Wassenaar Arrangement in its export laws, a company in Italy was actively selling and supporting intrusion software to foreign governments in the exact way that the arrangement was designed to prevent.

It is clear to us that BIS is trying to put in place rules with the right intentions. However, after reviewing the proposed rules, the BIS frequently asked questions, and summaries of conference calls held by BIS, the Internet Association believes that the rules in their current form could have a negative impact on our ability to defend our networks from attackers.

Before describing our concerns with the proposed rules and our recommendations, it is important to provide some background on the various methods our member companies use to improve the security of our own systems. By describing our general approach to security, we believe we can help BIS develop a better understanding of a complex and highly specialized discipline.

¹ The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits and Zynga.



2. How Internet Association Members Assess Security

In the broadest sense, approaches for assessing security of systems can be placed in two categories: process-focused assessments and technology-focused assessments. Process-focused assessments evaluate the **implementation** of security controls and their supporting processes by determining if they are in place and operating effectively. These are often non-technical assessments against a recognized standard such as the Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (aka SOC2), International Organization for Standardization 27001/2, or various National Institute of Standard and Technology (NIST) frameworks. These assessments determine whether controls are operating as expected based on their design.

Technology-focused assessments evaluate the **effectiveness** of controls, often by simulating the same approach an attacker takes to break into a network or systems. These assessments can take a number of forms including, but not limited to:

- *Internal/external vulnerability scanning*: where a security practitioner uses automated tools to identify potential vulnerabilities based on non-intrusive signatures. These scans are generally focused at the infrastructure layer (e.g. the operating system and common network services such as web server software and database software).
- *Internal/external network penetration testing*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities and attempt to exploit them to gain unauthorized access. As with internal/external vulnerability scanning, these assessments are often focused at the infrastructure layer.
- *Application assessments*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in a specific application and attempts to exploit them to gain unauthorized access. These assessments are often used to evaluate security on custom-built applications.
- *Source code reviews*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in the source code of a specific application. As with application assessments, these assessments are often used to evaluate security on custom-built applications, generally in combination with a broader application assessment.
- *Red team/Blue team exercises*: These exercises are the most open-ended form of security assessment and they most closely simulate a real-world scenario. During these exercises, security practitioners (called the “red team”) use a combination of automated and manual tools to identify vulnerabilities across an entire environment and attempt to exploit them to gain unauthorized access. Meanwhile, other security practitioners (called the “blue team”) attempt to detect the red team, investigate their activities, remove them from the environment, and exfiltrate data from the network. Throughout these exercises, the red team may, under company policy, have legitimate and legal access to data relevant to the exercise that is needed to prove its success and/or to gain additional access.
- *Bug Bounties*: where a company pays independent security researchers from outside of the company to identify and report vulnerabilities in a system, allowing the company to crowdsource the identification of vulnerabilities. The researchers who report these vulnerabilities can be from anywhere in the world.



While different companies may use a different combination of these assessments, most companies recognize the value provided by each type of assessment and tailor their security programs around them.

3. How Security Software Tools Support Company Assessments

Security software tools play a critical role in helping make security assessments more effective by improving security practitioners' capabilities in a number of ways, including:

- *Automation and Speed:* Many companies, especially the members of the Internet Association, have large infrastructures including hundreds of thousands of servers and hundreds of network services. There is no way to perform assessments of these large infrastructures without the automation and speed that these tools provide. Manually evaluating the susceptibility of each service, on each server, for each potential vulnerability is impossible.
- *Scale:* While related to automation and speed, scaling is important to call out individually. These tools not only let companies scale to the size of their environments but also let companies scale their talent. Using effective security tools allows a company to make a practitioner more effective by having them cover a wider breadth of systems and services. Given the difficulty in hiring talented security practitioners, scaling the ones we have is critical to supporting security in large environments.
- *Proof and Validation:* Once a practitioner finds a potential vulnerability, they achieve the best results from their efforts when they are able to validate the real risk of the vulnerability, not just the perceived risk. There is a significant difference in impact when a practitioner is able to say “this is what I was able to do” as opposed to “this is what I **may** be able to do.” The best way to validate the real risk of the vulnerability is to exploit it.
- *Simulation:* As explained above under “Red team/Blue team exercises”, the maximum value a security practitioner can bring is through the simulation of a real world attack. “Software” “specially designed” or modified to avoid detection by “monitoring tools,” or to defeat “protective countermeasures” of a “computer or network-capable device” describes tools that attackers use every day. A practitioner cannot simulate a real attack without using these types of tools.

4. The Value of Information Sharing

In addition to conducting assessments, companies often share information about emerging threats. This allows all participating companies to benefit from the efforts of a single company and respond to these threats more quickly. This information sharing happens in a number of ways including through commercial platforms, email lists, conferences, forums, and open platforms such as ThreatExchange (<https://threatexchange.fb.com/>). The latter platform is hosted by Facebook, an Internet Association member, and is used by a number of other Internet Association members, including Coinbase, Etsy, Google, LinkedIn, Netflix, Pinterest, Salesforce, Twitter, Yahoo, and Yelp, with more companies in the process of onboarding. Often, the information we share includes exhaustive details of tools, techniques, and procedures (TTPs) that we have seen attackers use within our networks. Sharing this level of detail maximizes the value of these exchanges.

As information sharing among organizations has grown, the value of this information sharing has grown as well. Many companies now view this as an integral part of their ability to detect and respond to new



threats. In fact, the U.S. government has recognized the value of this sharing as well, with President Obama issuing Executive Order 13636, “Improving Critical Infrastructure Cybersecurity”. (See Section 4 of the Order, stating “It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.”)

While we have seen an expansion in information sharing, the industry still has a very long way to go. Most companies are not actively sharing information or have limited information sharing capabilities. In the coming years, it is critical that we focus on doing everything we can to encourage broader information sharing (subject to appropriate privacy protections) across the industry.

5. Concerns with the Proposed BIS Rules

In light of the ways in which Internet Association member companies assess their security and the value of the threat information they share, they have a number of concerns with the proposed BIS rules:

1. **There is no intra-company exception built into the proposed rules.** As a result, companies may run afoul of the rules simply by sharing software or tools that leverage exploits for testing and validation purposes within their own teams. For example, some items controlled under the proposed rules would no longer qualify for License Exception ENC, which allows for intra-company transfers.
2. **The proposed rules are broad, ambiguous, and open to interpretation.** The ongoing discussions and clarifications are evidence of how difficult the proposed rules are to understand in their current form. To date, the clarifications have addressed specific examples or identified use cases, and have not effectively refined the broader context or scope of the proposed rules.
3. **In areas where the proposed rules are clear, they create a significant regulatory burden.** Any organization that wants to develop tools that would be controlled under the proposed rules will need to implement new or updated export control processes, which will incur additional costs and increase time to market. In addition, the proposed rules create enormously complex hurdles for individual researchers who might otherwise be able to make a meaningful impact on overall security.
4. **The proposed rules would have a chilling effect on information sharing and collaboration.** Companies and researchers might elect not to share information, even if permitted by the proposed rules, due to the difficulty in understanding their restrictions. This chilling effect will be felt most strongly by independent researchers or small security companies who may lack the resources or legal support to understand and comply with the proposed rules. The ambiguity of the proposed rules only adds to this chilling effect.
5. **The proposed rules would limit a company’s ability to employ non-U.S. resources in security-related activities.** Restrictions on information sharing within a company would limit the ability of companies to attract and retain well-qualified non-U.S. employees, whether in the U.S. or elsewhere, in security-related roles by requiring companies to assess citizenship and nationality and obtain export licenses in order for these employees to access controlled technology and source code. This problem would be most salient in the use of cross-border red/blue teams, but it would also arise even if entirely U.S.-based teams were used, due to the operation of BIS’ long-standing “deemed export” rule. In order to avoid these costs and added



layers of complexity, companies might have to forgo hiring the best and brightest security experts, ultimately harming their cybersecurity.

6. **Similar rules have not worked in the past.** In the technology space, the existing rules around export of encryption technology have done little to limit the proliferation of the technology, which has resulted in a series of revisions to BIS encryption rules as the government attempted to keep pace with rapid developments in the marketplace. The proposed rules appear to be taking the same approach to a similar problem, rather than rethinking this unsuccessful approach and developing a new model to address the proliferation of intrusion and surveillance items.

6. How the BIS Rules would Impact Companies' Ability to Improve Security

Our analysis of the proposed rules has identified a number of ways in which they could, as currently drafted, negatively impact our member companies' ability to improve their own security. Provided below are some real world scenarios that illustrate this negative impact.

Impact on Security Assessments

The proposed rules would have the most direct impact on red team/blue team exercises. These assessments simulate real-world attacks by using the same TTPs that attackers use, actively compromising systems, and exfiltrating data to test defenses. The red and blue teams could be located in multiple countries. The proposed rules would cripple our ability to perform red team exercises using non-U.S. resources because we might not be able to perform exfiltration of company-owned data from company-owned systems without first obtaining an export license. This would hinder our ability to rapidly test systems in response to the discovery of a new vulnerability. Likewise, the effectiveness of blue team exercises may be limited by our inability to share certain information and tools internally with non-U.S. resources without first obtaining an export license.

Impact on Security Tools

The most obvious impact on security tools from the proposed rules will be increased cost. Commercial companies that develop tools affected by these proposed rules will need to increase the cost of their tools to offset the additional cost of the regulatory burdens they impose. Since there is no intra-company exception in the proposed rules, if any of these companies have engineering resources based in locations to which they cannot export their own software without first obtaining an export license, they may have to relocate engineering positions to new and potentially more expensive locations. Many of these costs will be passed on to their customers in the form of increased prices for purchasing licenses. In addition, consulting firms that use similar tools will pass on this cost to their clients in the form of increased consulting fees for security consulting engagements.

There is also the potential for decreased variety and capability of available security tools. Increased cost and reduced speed to market for these tools may force commercial vendors to rethink their product portfolios to reduce their regulatory burdens. In addition, obtaining export licenses for items controlled by the proposed rules will increase the time required to release new capabilities in these tools. These delays could prove harmful, given the race to fix vulnerabilities once they are known to the public. Restrictions on the export of these tools to certain destinations could also hinder efforts to



mitigate security risks, potentially undermining the policy goals of the proposed rules by creating a new class of “soft” targets.

Impact on Information Sharing

The proposed rules will negatively impact both inter- and intra-company information sharing. The proposed rules make inter-company information sharing far more complex and much less effective. To avoid exporting controlled items, companies will need to determine the location and nationality of any company or individual with which they want to share information as well as determine which information is controlled and cannot be shared. Additionally, while it may be possible to determine in advance the companies or individuals with which a company wishes to share information, by their very nature the information or tools to be shared cannot be determined in advance, because the threat cannot be determined in advance. Thus, proactive steps to establish information sharing channels before a crisis occurs are precluded by the proposed rules. Given the need for growth of inter-company information sharing, any regulations that discourage information sharing are cause for significant concern.

For intra-company information sharing, the proposed rules make it nearly impossible for our U.S.-based incident response teams to share fully detailed threat information with company security operations center (SOC) personnel outside of the U.S. Sending security or testing tools related to these new threats may constitute an export requiring a license, even if it is only intended for defensive purposes. For example, if a U.S.-based incident response team discovers details on a new exploit and exfiltration software being used against its systems, it may not be able to send needed tools to incident response teams in Israel without first obtaining an export license. If the U.S.-based team applies for a license, critical systems may remain vulnerable while waiting for BIS to process the application.

Impact on Bug Bounties

One of the pieces of technical information that often comes from bug bounty reports is proof of concept software or tools that can be leveraged to validate the vulnerability. This essential technical information may constitute tools that are covered under the new rules. For example, when a researcher provides us (or we provide a software vendor) with a proof-of-concept exploit and additional technical data that outlines the underlying issue, steps of exploitation, and how the vulnerability might be used in a real attack, we are creating tools covered by these rules, even though our explicit intent is to help improve defenses. Without this complete, accurate, and full picture of a vulnerability, we cannot begin to secure our systems and software. Many of the vulnerabilities we receive are highly complex and difficult to reproduce. Thus, a usable bug bounty report might not just require information about the vulnerability, it might require the provision of software “specially designed” for the generation, operation or delivery of, or communication with “intrusion software” in order to demonstrate how a vulnerability could be exploited by an attacker. If we do not receive such tools, we may be unable to reproduce the vulnerability or validate that a designed patch actually addresses it.

In addition to limiting the data provided in bug bounty reports, we fear that the proposed rules would have an overall chilling effect on researchers' willingness to participate in these programs, whether due to actual licensing requirements, or due to widespread misconceptions over what kinds of tools and information are controlled under the proposed rules. As recent coverage in the trade press indicates,



many security researchers believe that sharing information on exploits is prohibited under the proposed rules, even though BIS has repeatedly stated that this is not correct. This chilling effect would lead to a direct reduction in the effectiveness of bug bounty programs. (See, e.g., “Student Claims Wassenaar Arrangement Prevents Him from Publishing Dissertation,” *Ars Technica*, July 2, 2015, available at: <http://arstechnica.com/security/2015/07/student-claims-wassenaar-agreement-prevents-him-from-publishing-dissertation/>; “Arms Control Treaty Could Land Security Researchers Like Me in Jail,” *Ars Technica*, May 27, 2015, available at: <http://arstechnica.com/security/2015/05/arms-control-treaty-could-land-security-researchers-like-me-in-jail/>)

How the Proposed Rules can be Improved

Since introducing the proposed rules, BIS has taken steps to clarify its position, but its interpretations of the proposed rules still remain unclear. For example, some of the FAQs appear to contain contradictions. As explained by the Electronic Frontier Foundation, “FAQ 10 clarifies that a researcher who has written a proof of concept for a vulnerability, 'code that takes advantage of the vulnerability,' would not be required to obtain a license before submitting the proof of concept to the vendor. But back up in FAQ 4, BIS told us that 'information on how to prepare the exploit for delivery' is controlled.” In addition, responses during conference calls show that BIS is still working to understand this space. We applaud BIS for noting that they are still gathering information about the industry; however, we believe that regulating such a complex industry without a deep understanding of how all of its pieces fit together is a dangerous approach.

Industry's reaction to the proposed rules demonstrates that, while BIS has good intentions, the proposed rules will have a number of unintended consequences. If BIS feels that it must regulate these tools, it should write the rules as narrowly as possible and with the goal of minimizing their adverse impact on the following key items:

- Inter and intra-company information sharing;
- Legitimate research that helps identify and fix vulnerabilities in the systems, software, and networks we use every day;
- Bug bounty and other similar programs that help businesses secure their systems, software, and networks with the help of vulnerability researchers;
- The need of companies and individuals to use security software to identify vulnerabilities in their own systems, software, and networks;
- The power that comes from researchers producing detailed reports on vulnerabilities to help developers fix their software; and
- Additional costs that will be incurred by companies and individuals who want to use security software to secure their systems, software, and networks.

To help address the concerns raised in this public comment, the members of the Internet Association recommend the following steps to bring the proposed rules in line with the harm we believe they are truly meant to target (*i.e.*, illegal surveillance and exfiltration of data from a target without authorization):

1. Introducing an intra-company exception;



2. Focusing on exfiltration and the use of cybersecurity items for unauthorized activities, not the items' technical capabilities;
3. Maximizing clarity around acceptable uses that do not require a license;
4. Including more detailed language in the regulations' text and preamble, similar to what has been included in the FAQs;
5. Sharpening the definition of “Intrusion Detection Systems” to include technologies that are both system and network-based, in order to avoid conflating network intrusion detection systems (NIDS)/man-in-the-middle (MITM) tools with surveillance tools; and
6. Providing better and more comprehensive guidance to help individuals and organizations understand their obligations under the proposed rules.

Respectfully submitted,

Michael Beckerman
President & CEO
Internet Association

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k38-knb3
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0144

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jim Wojno

Address:

1159 Bolich Drive

Wadsworth, OH, 44281

Email: jim_wojno@yahoo.com

Phone: 3303317609

General Comment

While the proposal of controlling intrusion software, attack kits, network intrusion tools, network traffic analysis tools, spyware and other tools that can be used for malicious purposes is a laudable goal this attempt to do so is incredibly naive, shortsighted and ultimately doomed to failure.

All this new proposal would accomplish would be to make legitimate security research potentially criminal and that make it that much harder to perform. Far from making us safer - this would make us much less safe.

Currently, security researchers from around the globe routinely collaborate on projects and alert each other to 0 day exploits through social media and other collaboration environments. This strengthens the entire community as it allows everyone to immediately understand not only that a threat exists, but potentially what it's impact is, how to mitigate it, when (or if) a patch will be released to resolve it and who the primary people are that are driving the investigation and remediation efforts. Some fantastic examples of this process in action are recent events such as heartbleed, shellshock and the most recent Hacking Team 0 day Adobe exploits.

Note that in all of these events, the free flow of critical technical information across country borders was necessary to leverage the entire community - and in doing so the entire community benefited. Had artificial delays been introduced in order to ensure compliance with this agreement, this would have only benefited malicious threat actors who would have been free to continue using these exploits (and sharing them freely) while the legitimate security community ground through needless red tape.

Note that with regards to the Hacking Team 0 day disclosures, since HT would have been considered a licensed and approved supplier of these dual use technologies the changes being proposed would not have prevented anything that happened. It would not have prevented HT from developing the exploits it used and provided it's customers - since those customers were mainly governments. It would not have prevented dangerous security vulnerabilities from existing in the first place. It would not have prevented black hat / criminal hackers from using these vulnerabilities in their campaigns. It would not have protected political dissidents or other vulnerable people / groups from these exploits and the subsequent spying they enabled. Nothing would have been prevented except the identification, verification, testing, discussion and open collaboration on finding remedies for these exploits by the larger multi-national security community. Only legitimate research and defense would have been hampered.

The proposal is far too broad and appears to have been drawn up to control non-digital technologies such as weapon manufacturing devices. Such devices can be easily controlled since they are not portable, come only from a small number of providers and require not only specialized implementation and transportation but also specialized maintenance and replenishment parts.

None of this is true for dual purpose digital technologies.

This approach was tried in the 90's with the attempt to exert export control on encryption technologies and all it accomplished where the following:

- 1.) It forced adopted technologies to be purposely inferior to meet the artificial caps on bit count and hence made these technologies far less effective
- 2.) It forced development of more effective technologies off shore and outside the US

Note that at no time where criminals, rogue governments or terrorist ever impacted by those restrictions - only lawful users and developers were impacted.

There are already overly vague laws pertaining to security research which make the task difficult and at times dangerous; we do not need to make this situation worse.

A case in point is what happened to Andrew Auernheimer after he released information about AT&T's unsafe practices with customer sensitive data. He should have received accolades for making the community aware of such dangerous practices on AT&T's part but was instead imprisoned. The fact that his prison sentence was overturned does not address the very real cooling effect his conviction had on security research. There are many other scenarios like this - too numerous to list here - but the point remains that we need to encourage security research - not silence it.

This is an incredibly misguided attempt to exert controls which were developed for physical technologies on digital technologies and those controls are wholly unsuited for this. The end result of this - if adopted - is to make our systems and networks far less secure for questionable gain and to further erode the US as the global center of technological innovation.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-kxgv
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0145

Comment on FR Doc # 2015-11642

Submitter Information

Name: Cheri McGuire

Address:

700 13th Street NW

11th Floor, Suite 1150

Washington, DC, 20005

Email: governmentaffairs@symantec.com

Phone: 202-383-8700

General Comment

See attached file(s)

Attachments

Symantec Wassenaar Cyber Rule Comments 07202015



July 20, 2015

Ms. Catherine Wheeler
Director, Information Technology Control Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49) Published in 80 Fed. Reg. 28853 on May 20, 2015

Dear Ms. Wheeler:

Symantec Corporation (Symantec) appreciates the opportunity to provide comments on the proposed rule published by the U.S. Department of Commerce Bureau of Industry and Security (BIS) on May 20, 2015 in the Federal Register titled *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*. We have significant concerns about the proposed rule and the negative consequences it will have on the security industry and our customers. While the rule may have been designed to cover “intrusion software” used to breach systems, its broad language will affect a wide array of legitimate cybersecurity research and network penetration testing tools. As such, implementation of the proposed rule will stifle legitimate vulnerability research and the ability of Symantec and other companies to protect their own networks, and those of their customers.

While we recognize that the rule was intended to protect national security interests and preserve human rights, it misses the mark. It presupposes that systems, equipment, components and software that are specially designed or modified for the generation, operation, or delivery of, or communication with, “intrusion software” are “hacking” tools that are *all* used for nefarious purposes. This is not the case. In fact, Symantec – and virtually every other legitimate security company – uses such tools to ensure the security of our networks and commercial products.

In its current form, the rule would have far-reaching and detrimental effects on the cybersecurity industry and on cybersecurity writ large. It would severely damage legitimate vulnerability research and security testing worldwide, and thus undermine our ability to protect our own networks and to develop new and innovative cybersecurity products and services. The result would be that the end-users of security products – businesses, governments and individuals – would be less secure and at greater risk.

The proposed rule would harm the cyber security industry in three significant ways by:

- Restricting access to legitimate cybersecurity technologies and testing tools across borders – *even among security professionals who work for the same company.*

- Curtailing research into cybersecurity vulnerabilities, as researchers would be hindered from testing networks and sharing technical information across borders.
- Limiting cybersecurity threat information sharing and collaboration on cybersecurity risks both within security companies and with customers and industry partners, as information would be deemed “exported” if it is shared with *any* non-U.S. persons even if they are physically located in the U.S and employed by a U.S. company.

Symantec is a global security company with researchers based in several countries. Because of its breadth, the proposed rule could require our American researchers to obtain a government license in order to have anything more than a cursory conversation about new security vulnerabilities and exploits with any co-worker who is either not a U.S. citizen or who is situated outside the U.S. (even if that foreign-based employee was a U.S. citizen). Moreover, because the proposed rule does not distinguish between nefarious hacking tools and legitimate network security products commonly used for commercial penetration testing, we would need a new license every time we conduct defensive network or product testing outside the U.S. It is important to note that testing is done on a continual basis, so the delays associated with such licensing would create not only a heavy administrative burden, but also increase our risk of attack.

Finally, the rule would cripple our ability to share cyber threat and vulnerability information. This has long been a priority of the U.S. government, yet the proposed rule would have a chilling effect on the security community writ large as sharing details about vulnerabilities and exploits with experts outside the U.S. could be prohibited without first obtaining an export license. Drawing restrictions broader than is necessary simply to cover malicious tools will not limit, to any effective degree, the transfer of nefarious hacking tools. It would only bolster cybercriminals and rogue regimes as it would hamstring research to detect and provide protections against their illegal activity.

The BIS should withdraw this proposed rule and negotiate revisions to the language agreed upon at the 2013 Wassenaar Plenary Meeting. Absent such action, the BIS should revise the rule as discussed below to limit the harm to legitimate security testing and research, and to cybersecurity overall.

Introduction to Symantec

Symantec (www.symantec.com) is a U.S. corporation and is a global leader in providing security, storage, and systems management technology solutions to help businesses, governments, and consumers secure and manage their information. Founded in 1982, and headquartered in Mountain View, California, Symantec has operations in 50 countries, with more than 20,000 employees, and is the fourth largest independent software company in the world. Our unique focus is to minimize risks to information, technology and processes independent of the device, platform, interaction or location.

Penetration Testing Overview

To understand how the proposed rule will harm cybersecurity, it is necessary to understand a common security tool known as penetration testing (often referred to as “pen testing”). Penetration testing is a suite of tests designed to stress the target system (as real attackers would) in its operating environment. Penetration testing also is used to evaluate the security of a system or software product by analyzing its weaknesses and trying to compromise it. It is best done in a highly controlled environment using specialized computer systems and as part of a broader security testing strategy.

At commercial companies, typically there are two primary categories of penetration testing:

- (1) Pre-production penetration testing which is done on products or a family of products before they are released for sale to customers; and
- (2) Post-production penetration testing where testers operate on a much broader scope and ensure corporate networks and systems are secure.

In pre-production penetration testing, there usually are three types of penetration tests: black-box, white-box, and gray-box. In a black-box assessment, the testers have no information prior to the start of testing. In a white-box assessment, they will have complete details of the network and applications. For gray-box assessments, the testers will have some details of the target systems. Symantec typically performs gray-box assessments on its own products as this type of assessment yields more accurate results and provides a more comprehensive test of the security posture of the environment than does a black-box assessment.

In post-production penetration testing, testers take a much broader scope in their targeted systems and approach to penetration. This process is, at all times, carefully managed, scoped, and monitored so that any dangerous vulnerabilities discovered are carefully guarded and not allowed outside of the network – or into the “wild”. While this testing is directed at our internal networks and systems, we also often discover vulnerabilities in third party hardware and software that we use in our IT environment. When we do, we must notify the developer of the vulnerable product and work with them to develop a remediation. All data collected, vulnerabilities found, exploits researched and developed, and remediation fixes and approaches are kept strictly within a protected environment for complete safety.

Penetration Testing at Symantec

Penetration testing at Symantec is done primarily in two ways. First, it is used in the pre-production environment by our Software Security Group (SSG) prior to releasing a product to the market. The second way we do penetration testing is in the post-production environment by our Global Security Organization (GSO) in accordance with our own policies and best practices, and in response to industry mandated standards (e.g., PCI DSS, FedRAMP, FFIEC, etc.).

Pre-Production Penetration Testing

Symantec’s SSG provides security guidance and protocols to our software developers across the company to ensure they are delivering a secure product. The SSG works closely with the product teams to deliver training and guide them on software security best practices and best-of-breed tools.

The SSG-driven pre-production penetration tests are done as gray-box assessments. The penetration testers identify the most serious and critical security weaknesses, and direct the development quality assurance teams to the parts of the system that require attention and/or remediation. The SSG typically conducts more than sixty penetration tests a year.

The objective of pre-production penetration testing is to improve the quality of products by identifying weaknesses and flaws that can be remedied *prior to* the release of the product to the market. Ultimately, this type of testing helps ensure that Symantec delivers products with a high level of safety, security, and integrity.

Post-Production Penetration Testing

Symantec's GSO group conducts penetration testing in the post-production environment that spans all aspects of our infrastructure – from our worldwide networks and systems to individual products to corporate sites and data centers. The objective is to identify weaknesses or vulnerabilities at any level or part of Symantec and its development processes, and work to remediate those gaps.

Each post-production penetration test engagement is carefully scoped and planned with the organizations involved including the business leaders and engineers, developers, and technicians that typically span geographic boundaries. While target organizations are deeply involved in the planning and scoping of a testing engagement, they almost never are notified in advance of the actual test execution. In most cases, our penetration testing engagements are conducted in a covert fashion, and everything from the timeline to the end results are closely guarded corporate secrets.

A series of actions are taken to design and deploy the testing. First, application teams will generate a series of virtual machines and provide them to the penetration test team. This gives the test team a pre-configured environment of software on a virtual machine. Occasionally, an entire appliance is provided to the test team with pre-loaded software. In addition, the GSO penetration testers will test third party-provided software and hardware and systems, but always with permission of the third party. Thus, tests on some aspects of the targeted systems or networks would involve hardware and software not owned or developed by Symantec.

Second, once the scope of the engagement has been confirmed, the penetration testers use systems and software that are specially designed to find vulnerabilities through the development of technology, exploits and other tools. As noted above, the penetration testers will always operate out of an isolated and secure systems environment created specifically for penetration testing.

Third, the penetration test team will use hardware, software, applications, and bits of software code from any source available including those outside of Symantec. They will also write their own code to exploit vulnerabilities. All of these various pieces of hardware and software are assembled into a penetration "system". The penetration systems are built to provide the mechanism of testing for vulnerabilities, as well as to extract the data and document the vulnerability and various exploits used for research and technology purposes. An example of such a system could be a commercially available laptop to which a wireless router and some network switching gear are connected. The penetration tester may purchase some widely available software such as automatic exploit generators on the internet or from a retail outlet. They also may develop some custom exploit code on their own in order to fully stress the targeted system.

We believe that the proposed rule as written would cover all of the various aspects of the penetration system. This includes the pieces of hardware, software, applications, software bits, etc. that our penetration testers assemble into a command and control system to deliver, direct, and communicate with the intrusion software. These are all systems, equipment or software that is "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software" as set forth in proposed ECCNs 4A005 and 4D004.

Performing penetration tests both internally and for customer systems is a high risk process. Companies take extreme measures to ensure that vulnerabilities and exploits do not leak outside the secure testing environment. Because of the risk, it is also critical that the testers themselves are highly trained and

experienced in penetration testing. Members of Symantec's penetration testing team have years of experience conducting physical, network, and application penetration testing against large environments and possess industry certifications, including those directly related to technical penetration testing. This high level of experience means Symantec penetration testing teams are conducting comprehensive testing engagements internationally, and targeting various industries to include, but not limited to SCADA, healthcare, financial, government, commercial, and non-profit.

General Comments on the Proposed Rule

New Category 4 ECCNs and Executive Order 13691

Unfortunately, the control on intrusion items in the proposed rule will cover tools used by Symantec and other legitimate security companies for routine penetration and security testing. The proposed rule therefore would limit the ability of security companies to share technology or technical data related to cybersecurity risks, both within a company and with customers who hire security testers. This would make industry's efforts to ensure the security of information technology products slower, more costly, and less operationally effective.

Specifically, the proposed rule would control systems, equipment, components (4A005) and software (4D004) that are specially designed or modified for the generation, operation, or delivery of, or communication with, "intrusion software". It also would control technology (4E001.a) if required for 4A005, 4D004.a (if required for 4A005 or 4D004) and if required for 4E001.c. The relevant part of the Supplementary Information section of the Proposed Rule at page 28854 reads:

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.

In FAQ #1, the BIS noted that, "A penetration testing tool not designed to avoid detection by 'monitoring tools' would not be controlled". But this ignores the purpose of penetration testing, to replicate the tools, techniques, and practices of malicious attackers. The tests conducted by Symantec's GSO, for example, are designed to avoid detection and are conducted in a covert fashion – a critical component of the test in order to be as effective as possible.

Because Symantec conducts penetration testing in various locations around the world and sometimes employs specialized vendors, the proposed rule would place onerous restrictions on our security work. The fact that this work is done by Symantec largely for its own security purposes does not put us outside the reach of the control, as is described in FAQ #17:

Under the proposed rule, all exports of specified systems, equipment, components or software that would generate, operate, deliver or communicate with "intrusion software" would require an export license. There is no license exception for intra-

company transfers or internal use by a company headquartered in the United States under the proposed rule.

The lack of a license exception for intra-company transfers or internal company use will result in hundreds of deemed export license applications, a large number of technology transfer licenses, and a large number of licenses for systems, equipment or software "specially designed" or modified for the generation, operation or delivery of, or communication with, "intrusion software". This will severely limit Symantec's ability to continue conducting the robust testing done today – and put our corporate networks, employees, and customers at heightened risk.

The Proposed Rule also undermines the U.S. government's efforts to increase cyber information sharing among private companies. On February 20, 2015, the President signed Executive Order 13691 titled "Promoting Private Sector Cybersecurity Information Sharing" [80 Fed. Reg. 9349]. It reads in part:

Section 1. Policy. *In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.*

Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.

Presumption of Denial Related to Rootkit or Zero-day Exploit Functionality

In the preamble to the proposed rule, in the section titled *License Review Policy for Cybersecurity Items*, it states:

Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.

The presumption of denial for licenses related to zero-day exploit functionality is highly problematic. Simply put, not every rootkit or zero-day is shared for malicious purposes; we do so in order to fix these dangerous vulnerabilities, not to exploit them. Indeed, these zero-day vulnerabilities and exploits are the very items that companies seek to find and deal with in their penetration testing engagements and exercises. The inability to freely share this information and the related research and development of defenses within our company will severely impact our ability to create safe products and ensure a secure network and IT environment.

To the extent that the BIS intends to maintain distinct, restrictive licensing policies for rootkits and zero-day exploits, it should provide specific definitions for those terms. In the alternative, the BIS should consider whether rootkits and zero-day exploits fit the definition of "intrusion software," and therefore would not be controlled under the proposed rule. In turn, this would not require a licensing policy. If

rootkits and zero-day exploits are defined as "intrusion software," the BIS must provide clarification in the next version of the rule, not solely in a non-binding FAQ.

Industry Mandated Testing

Certain industries are legally required to conduct penetration testing and other industries have implemented this type of testing as part of their industry standards and best practices. Among these are the financial services, healthcare, and power industries as described below. Under the proposed rule, companies using testing tools and processes to comply with regulatory requirements and industry standards will need to implement costly and time consuming changes to their internal compliance programs in order to obtain the necessary export licenses. The unintended consequences of this proposed rule will mean weaker security and more frequent security breaches across critical infrastructure sectors.

Financial Services Industry

The financial services industry has unique information security requirements. A frequent target of attacks, banks perform a high level of due diligence to ensure the confidentiality, integrity and availability of customer transactions. Penetration testing is one way to stress the attack surface that an organization presents to the outside world. Financial industry regulatory guidelines that include a reference to penetration testing include the following:

- The Federal Financial Institutions Examination Council (FFIEC) guidance on independence tests (<http://ithandbook.ffiec.gov/it-booklets/information-security/security-monitoring/condition-monitoring/independent-tests.aspx>) describes the value of penetration testing:

A penetration test subjects a system to the real-world attacks selected and conducted by the testing personnel. The benefit of a penetration test is that it identifies the extent to which a system can be compromised before the attack is identified and assesses the response mechanism's effectiveness. Because a penetration test seldom is a comprehensive test of the system's security, it should be combined with other monitoring to validate the effectiveness of the security process.

- The Payment Card Industry (PCI) Data Security Standard (DSS) details security requirements for merchants and service providers that store, process, or transmit cardholder data. To demonstrate compliance with the PCI DSS, merchants and service providers may be required to have periodic PCI Security Scans conducted as defined by each payment card company. The PCI DSS Security Scanning Procedures include requirements for penetration testing. These are found in: Information Supplement: Requirement 11.3 Penetration Testing, March 2008; and Information Supplement: Penetration Testing Guidance, March 2015.

Power Industry

Addressing cybersecurity is critical to enhancing the security and reliability of the nation's electric grid. Ensuring a resilient electric grid is particularly important since it is one of the most complex and critical infrastructures that other sectors depend on to deliver essential services.

- The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards. All bulk power system owners, operators, and users must comply with approved NERC reliability standards. The NERC's Critical Infrastructure Protection standard (CIP-007) describes the requirements related to testing procedures for malicious software prevention, account management, system event monitoring, disposal or redeployment, vulnerability assessment, and documentation.
- The National Electric Sector Cybersecurity Organization Resource (NESCOR) has created a security test plan template to provide guidance to electric utilities on how to perform penetration tests on Smart Grid systems. NESCOR's goal is to protect the electric grid and enhance the integration of smart grid technologies that will mitigate the effects of cyber-attacks – both malicious and non-malicious. [<http://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf>]

Healthcare Industry

The healthcare industry faces heightened privacy and security concerns associated with the electronic transmission of health information among health care entities. The Health Information Technology for Economic and Clinical Health Act (the HITECH Act) was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA) to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act, sections 13400–13424, addresses the privacy and security concerns associated with the electronic transmission of health information. It does so, in part, through several provisions that strengthen civil and criminal enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules.

- On January 25, 2013, the Department of Health and Human Services published a final rule that strengthened the privacy and security protections established under HIPAA for individual's health information maintained in electronic health records [78 Fed. Reg. 5566]. These enhanced security protections include the testing of networks to ensure they are safe.

Recent Security Breaches

The proposed rule does not distinguish between tools developed for and used by legitimate security companies from those employed by malicious hackers. In order to distinguish between tools used for legitimate purposes and those used for malicious purposes, intent must be established. A tool may be used by a law-abiding organization to identify vulnerabilities and prevent cyber attacks. The same tool could also be used for criminal or other nefarious purposes. Imposing a blanket licensing requirement would only impact the companies using the tools for legitimate purposes – they would have to implement significant changes to their internal compliance programs and obtain numerous export licenses. Criminals and “black hat” hackers^[2] probably will not know about the export rules, and certainly would not bother obtaining the required export licenses if they did know. Thus the proposed rule will negatively impact and significantly increase risk for all commercial companies that rely on continuously updated cyber defenses, while doing nothing to slow criminals.

^[2] A *black hat hacker* is a *hacker* who "violates computer security for little reason beyond maliciousness or for personal gain" (R. Moore, *Cybercrime: Investigating High Technology Computer Crime*, 2005, Matthew Bender & Company, p258).

The unintended consequences of this proposed rule will mean easier targets and more frequent security breaches such as the high profile ones in government, industry and academia that are in the news every week. The proposed rule will do nothing to curtail the underground market where criminals buy and sell exploits, vulnerabilities, and attack kits. What it will do is make it harder for U.S.-based organizations with operations around the world to deploy the best tools available to find the weaknesses in their own systems and to patch them – before an attacker does.

Responses to BIS Questions

In the proposed rule, the BIS asked about its effects and for answers to the following questions:

1. *How many additional license applications would your company be required to submit per year under the requirements of this proposed rule?*

Symantec would need a minimum of 85 licenses to conduct pre-production and post-production testing. In addition, we likely would need many more site licenses given the number of foreign subsidiaries and sites that participate in our standard testing programs. Equally as important, new licensing requirements would require the company to implement significant alterations to our internal compliance programs to obtain the necessary export licenses; these changes would require new resources and planning timelines for us to continue to operate a robust compliance program (e.g., hiring of additional compliance personnel and a 6-month lead time to collect the information necessary to submit an export license request).

The added burdens would negatively impact the ability of Symantec to be nimble and agile in responding to threats given that cyber attacks are constantly evolving and have no timeline. Further, it is not clear how we would write a license application given the fact that our penetration testing process is scoped to allow for detection of unanticipated vulnerabilities and additional follow on testing if needed. We envision a scenario where we conduct a test, find that we need to do more or different testing, and then must stop to wait months for another export license. In the meantime, our networks could remain vulnerable, or our product development and release cycles would be delayed. Both of these would have significant financial and market impacts on our business. For this reason, should the BIS not withdraw the proposed rule, it should at minimum revise it to:

- Create a license exception authorizing exports and deemed exports of controlled items relating to intrusion software when such exports and deemed exports are made:
 - to the producer of the vulnerable product wherever that manufacturer is located and its employees or contractors; or
 - to any other agent of the vulnerable product's manufacturer, wherever located; and
 - when the purpose of the export is to report vulnerabilities to manufacturers and to have the vulnerabilities be fixed.
- Create a license exception authorizing exports and deemed exports of controlled items relating to intrusion software when such exports and deemed exports are made by product manufacturers or their agents to individuals or entities that reported a vulnerability to them.

- Create a license exception for testing that is mandated by standards or regulations (e.g., PCI DSS, FedRAMP, FFIEC standards, etc.).

2. *Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.*

The rule would have significant negative effects on Symantec. "Intrusion software" as defined in the proposed rule would severely restrict our ability to conduct testing and vulnerability analysis on our products, systems, and development processes. This will significantly impact our customers as Symantec will be left with a choice to either do less testing or take much longer to deliver products and protections to our customers. Specifically, the proposed rule would limit:

- The sharing of information between Symantec employees or computers – indeed, across national borders and even across a single room – if someone within the U.S. shares technical data about security threats with someone who is not a U.S. or Canadian national.
- The development, operation, and functionality of automated security vulnerability identification and reporting tools, APIs, or backend systems, which Symantec builds into our products to defend our systems.
- The development and deployment of patches necessary to secure vulnerable products, leaving any system using that product vulnerable to hackers and criminals.
- The outside expertise and vendors that Symantec works with for cybersecurity and threat intelligence collection and analysis around the world.
- Information that Symantec shares across security and threat-sharing partnerships (e.g., information sharing and analysis organizations, computer emergency response teams, law enforcement, etc.).
- The sharing of threat information between Symantec and its customers.
- Information that is shared with the U.S. government voluntarily or as required under procurement contracts.

3. *How many deemed export, re-export or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?*

Symantec estimates that it would need to submit up to 850 deemed export license applications. We do not believe that the BIS has the capacity to process such a large volume of applications as currently staffed. The proposed rule represents an unknown, but significant licensing burden for the BIS. For this reason, should the BIS not withdraw the proposed rule, it should at minimum:

- Create an intra-company license exception authorizing exports and deemed exports of goods, software, and technology relating to intrusion software similar to the current intra-company provisions in license exception for encryption (ENC).

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

Symantec has an Encryption Registration Number (ERN) and the majority of our commercial products have been self-classified. However, our internal testing tools have not been classified. After reviewing the requirements in proposed paragraph (z) to Supplement No. 2 to part 748, we estimate it would take up to two weeks (80 hours) per product to answer the questions required to submit a license application. This is information that is not readily available or part of our standard internal documentation and would require significant effort and cost to develop.

Recommendations

For the reasons described above, Symantec believes that the proposed rule will have significant, negative consequences – to our business, our customers, and our internal operations. The BIS should withdraw the proposed rule, and negotiate revisions to the language agreed upon at the 2013 Wassenaar Plenary Meeting. Absent such action, the BIS should revise the rule, taking into account the recommendations below to limit the harm to legitimate security testing and research, and to cybersecurity overall.

- Create an intra-company license exception authorizing exports and deemed exports of goods, software, and technology relating to intrusion software similar to the current intra-company provisions in license exception ENC. When linked to the internal company penetration testing the license exception should extend to and include:
 - the producer of the vulnerable product wherever that manufacturer is located and to its employees or contractors; or
 - any other agent of the vulnerable product's manufacturer, wherever located; and
 - when the purpose of the export is to report vulnerabilities to manufacturers and to have the vulnerabilities remediated.

The scope of control on intrusion items should be strictly limited to platforms for launching attacks and technology required for the development of those platforms *if the platforms are not used by companies for legitimate testing*. The control should also exclude tools that are commercially available for testing the robustness of products and firewalls. Legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using intrusion items, should not be considered within the scope of this control.

- Exempt security vulnerability technology and software from the scope of the Export Administration Regulations (EAR), when it is shared with the intent to defend against possible attacks. In the alternative, the BIS should create a license exception authorizing the export of security vulnerability information, without pre-export review or post-export reporting requirements.
- Exempt security vulnerability technology and software from the scope of the EAR, when it is used for testing that is mandated by standards or regulations. In the alternative, the BIS should create a

license exception for testing that is mandated by standards or regulations (e.g., PCI DSS, FedRAMP, FFIEC standards, etc.).

- Provide specific definitions for the terms “rootkits” and “zero-day exploits,” to the extent that the BIS intends to maintain distinct, restrictive licensing policies for them. In the alternative, the BIS should consider whether rootkits and zero-day exploits are "intrusion software," and would not be controlled under the proposed rule; thus, not require a licensing policy. If rootkits and zero-day exploits are deemed to be "intrusion software," the BIS should provide clarification in the next version of the rule.

Thank you for the opportunity to comment on the proposed rule. Symantec would be pleased to provide additional information or answer any questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'Cheri McGuire', with a long horizontal flourish extending to the right.

Cheri F. McGuire
Vice President, Global Government Affairs
& Cybersecurity Policy
Symantec Corporation

cc: Kevin Wolf, Assistant Secretary for Export Administration
Matthew Borman, Deputy Assistant Secretary for Export Administration
Hillary Hess, Director Regulatory Policy Division, Office of Export Services

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-zp3p
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0146

Comment on FR Doc # 2015-11642

Submitter Information

Name: David Aitel

Address:

1130 Washington Ave

Miami Beach, FL, 33139

Email: dave.aitel@gmail.com

Phone: +1-786-263-9749

General Comment

See attached file(s) (Both have the same text, but are in different formats - Word and .txt).

Attachments

BISComments

Cyber Regulation Comments (Immunity)

BIS Comments on BIS-2015-0011 (Cyber Regulations)

From:
Dave Aitel
dave@immunity.com +1-786-263-9749
CEO
Immunity, Inc.
July 20, 2015

INTRODUCTION

Thank you for taking comments on the proposed new Cyber rules for export control regulations coordinating with the Wassenaar Treaty. Immunity is a US-based corporation with offices in Crystal City, and Miami Beach, and has been in the penetration testing market for over a decade. Our customers include major financial institutions, social network engines, global manufacturing firms, and the US Government. We both sell some of the most commonly used penetration testing tools, and conduct commercial consulting for our customers in the area of software security.

Our experience in this area, stemming from our long history supporting the US Government (I started my career at the NSA), and our expertise selling to the Fortune 50, gives us a unique perspective on the proposed regulations.

As a first point, we want to show that it's hard to suggest language to replace parts of the regulations, especially when it is not clear what the goals of the regulation truly are and the underlying definitions of several terms are undergoing revision (for example "Deemed Export").

For example, although there are groups (Citizen Lab and Privacy International, etc.) who have pointed out that Hacking Team's RCS and Gamma International's FinFisher software have been used to hack journalists and activists, it's not clear that export control regulations can be even moderately effective at protecting activists in foreign countries. In particular, neither FinFisher nor Hacking Team's software is technically different from penetration testing software already on the market from multiple vendors (including Immunity), and Hacking Team, while an Italian company, is already be operating under Wassenaar regulations and has approval from the Italian government for selling its tools.

At the same time, there is also a thriving black market for intrusion tools, commonly known as "RATs" (Remote Access/Administration Tools) and "Exploit Packs/Kits" to compromise machines for botnets or other malicious use. Such systems have already been used by hostile regimes (notably Syria) to compromise activists. No amount of export control can stop this already existing foreign black market.

Defensive efforts can work though in some of these cases. As a case example, using Microsoft's free EMET tool, Malwarebytes Anti-Exploit, a ChromeBook, or a non-Jailbroken iPhone would have protected any of these activists from everything in the arsenal of FinFisher and Hacking Team, which cannot target these platforms.

However, it is also true that without physical security, there can be no cyber security - and these activists in other countries are vulnerable at all times to things being installed on their computers via the standard mechanisms of having to go through borders and customs controls, leaving their computers and phones in hotel rooms, and being unable to control their supply chain (i.e. having government intelligence officials sell them software, phones, and computers that are already under surveillance).

In other words, in addition to imposing a high cost on American companies selling and using penetration testing software and other security software that is swept up under these proposed regulations, the regulations cannot possibly achieve any meaningfully positive results.

OVERVIEW OF PENETRATION TESTING

Immunity was started in 2002 and sells CANVAS globally, which is one of several penetration testing products that covers network penetration testing, along with SILICA, which covers Wifi penetration testing, and INNUENDO, which fits into a burgeoning market for more advanced tools that tests APT-style lateral movement emulation. Other tools in the marketplace include Rapid7's Metasploit Pro, CORE Impact/Insight, and the Pwnie suite of tools. But there are literally dozens of commercial products that fit into the current definition of command and control systems that would be used to "generate" intrusion software.

Penetration testing, at its root and heart, is about discovering a ground truth. You say you have Anti-Virus, but is it really working? Your intrusion detection system is set up to scan for bad emails, but I just sent some, so did it alert you? I am exfiltrating your database from your network - is your IT team able to see that?

This ability to discover a ground truth is a vital part of building a company's security defenses. This is why it is required by PCI, HIPAA, various NIST standards, and of course, any competent security team's daily efforts. They require their toolsets and consultants to emulate all manors of threats, in order to determine if their defenses are adequate, from low-level hackers, to APT-grade teams.

Likewise, information security is an industry that changes quickly. What one day is done only by the most advanced nation state attackers, tomorrow is done by every criminal and therefore is a highly desired part of a penetration testing suite to detect, model, and demonstrate the threats before attacks occur. This makes is especially hard to design restrictive regulations that only target "Bad Actors". Keep in mind that one of the more popular web penetration testing

platforms, Havij Pro is, in fact, made in Iran. The US and her allies do not have a monopoly on this area of expertise.

Penetration testing software is also used often for training. Immunity has conducted our own training for over a decade based on CANVAS, but of course, there is a large industry of people conducting training at conferences like BlackHat to help make people aware of the implications of hacking when applied to all sorts of new industries. Without this training, it is impossible to build awareness, for example, in the critical infrastructure area. Everyone hears about what a hacker could do to a power plant or sewage system, but no news article on Ars Technica can replace the eye opening experience of bringing a group of industrial control system engineers into a room and teaching them how to do it themselves in a controlled environment. The proposed deemed export restrictions in particular are problematic for this very important practice.

Modern corporations are global and their information is global and because of that their information security requirements are global. Under the proposed regulations an employee of Ernst and Young, crossing into Mexico to test their branch office there with penetration testing software installed would be criminally liable.

The FAQ provided by BIS indicated that there are exceptions for tools which are freely available. For example, NMap, Metasploit's BSD licensed version, or the tools on the Kali penetration testing live-distro. But, aside from the obvious interest the US Commerce department has in promoting US commerce, there are legitimate technical reasons for limited use commercial replacements for open source, public technology. The primary reason for this is the validity of the test itself.

For example, while you can get public versions of the SAT test, you cannot get the test you are going to take before you sit for the exam. Likewise, privately sold penetration testing equipment can provide a much more objective ground truth for a defensive technology, without allowing them to "Game the Test" by building signatures for particular things in advance.

In the FAQ, BIS states:

A penetration testing tool not designed to avoid detection by 'monitoring tools' would not be controlled. Also, a vulnerability scanner, which just finds vulnerabilities in a system without actually exploiting them and extracting data, would not be captured by the proposed rule.

But vulnerability management and penetration testing are different things. Typically a vulnerability scanner will err very heavily on the side of false positives, which leaves a lot of work to go through manually by a security engineer. Penetration testing, on the other hand, errs on the side of false negatives. These tools are often used together to help winnow down and prioritize the vulnerability queue. This means that while you may conduct a Nessus scan to find vulnerabilities, in order to discern any value from that scan, you often have to feed it into a validation tool like CANVAS or Metasploit or CORE Impact. So the proposed rule, while not explicitly targeting vulnerability scanners, partially neuters their ability to be useful!

Likewise, what does it mean to be “Designed to avoid detection by monitoring tools”? In the case of penetration testing software, that is the definition of their duty. Without trying to test the efficacy of the monitoring tools, they are not providing a ground truth.

ISSUES WITH DEFINITIONS IN THE CURRENT PROPOSED WORDING

Oday

The Carnegie Mellon University CERT, which has a long history of leadership in the information security space, and is used heavily by the US Government, has produced a long document on the issues with the term “Oday” when used in a regulatory context.

This can be viewed here in its entirety:

<https://www.cert.org/blogs/certcc/post.cfm?EntryID=247>

To summarize both their position, and our own, “Oday” is widely known to mean “I wish I had known about it”. It is a term of respect and envy, but not of a technical nature of any kind. Putting this phrase in a regulation adds vagueness to the text in a way that cannot be reconciled. Even defining the term “exploit” is impossible. Exploits are software that does “something that an attacker would want to do” and beyond that, any level of specificity adds ambiguity but not meaning.

BIS says this in their FAQ:

BIS does not anticipate receiving many, or any, export license applications for products having or supporting zero-day capabilities.

But every sale of CANVAS, CORE Impact, or Metasploit Pro would essentially have this feature, even assuming there was a possible definition of what it meant to “support zero-day capabilities”. All software is modular - and most software in this space is sold in an interpretive language such as Python or Ruby, allowing endless modifications and user-customization.

Rootkit

It should be noted that CANVAS has included a simple “Win32 kernel rootkit” for many years. This is used to open up customer’s eyes about the fact that processes and files can be hidden at the kernel level. But a “rootkit” originally had nothing to do with the kernel. Rootkit originally meant software that would maintain and hide persistence on a remote computer. This can be anything - from a simple backdoor, to a hardware-assisted implant, to an SSH key left in a particular directory.

But there's no one meaning to the term "rootkit" or "backdoor" or any of a number of similar terms. For example, people often talk about "Database Rootkits" but these have no technical implementation similarity to traditional rootkits. For this, and other reasons, any regulatory language mentioning rootkits should be removed. It's interesting as well to note language that says "without the permission of the device's owner" as used in the BIS FAQ is a not drawn on technical matters, but purely legal and business matters. A government can claim that due to its sovereignty, it has "permission" to deploy anything it wants to any computer in the country. Companies can also claim very broad levels of "permission" based on employment agreements. Even software companies will claim very broad rights to someone's computer, as part of their End User License Agreement. Sony has installed and used Rootkits in the past based on exactly these terms.

Rootkits are Useful For Security

Going forward, rootkit technology is becoming more and more popular for advanced protective measures. This is because attackers are becoming smarter and defenders need to act covertly, even on their own networks. For example, if you think an attacker is operating on your mail server, you often want to remotely install an agent with a built in rootkit to that machine, so you can covertly monitor the hacker's behavior and interactions with the rest of your network.

Products such as Mandiant and CrowdStrike are leading the way in this area, but it will soon be a common-place aspect of security controls which provide advanced situational awareness on machines, even when attackers are trying to prevent you from doing so.

Of course, nothing technically differentiates these tools from the ones the attackers use, other than who is driving the controls.

Carrier-grade

While so much focus has been on the export control regulations around intrusion software, it is hard not to notice that the term "carrier grade" slipped into the surveillance software control. The phone call and FAQ on this issue failed to bring any clarity to a term that is meaningless marketing-speak. On the phone call they referred to a network sized for "city or country". This is unnecessarily vague. For example, every building in Miami Beach can access a 500Mb mesh network courtesy of webpass.net. There are, say, a couple hundred buildings in Miami Beach, a small US city. So is the lower limit on how "fast" a system can be 200*500Mb?

The dictionary definition of "carrier-grade" is simply that of reliability, not speed. And if we are going to delimitate capabilities based on speed, then we need to double the speed every year to accommodate Moore's law.

Likewise, it's not appreciated in the regulation how similar "IP surveillance" is to advanced intrusion detection and prevention. While today this capability may be a niche product, tomorrow it will likely be part of every company's holistic and strategic network situational awareness program. Our export control regulations should not stand in the way of valid defensive progress which we are using to help companies control network attackers, some of which are highly skilled.

Public/Vendors

The BIS FAQ on the Cyber regulation goes into detail on how they are trying to prevent individuals preparing conference talks from being restricted. In part this is done by defining material released to the public or to vendors as being OK, whereas information held privately would be restricted. But the course of research is not a straight line. There are a number of extremely dangerous follow-on effects with this proposed regulation plan.

For example, assume you are a security researcher who finds a vulnerability the web server that runs in a Linksys router. Who do you report that vulnerability to? Linksys? The company that sold software to Linksys and many other vendors that is their base operating system? What about a company that uses this Linksys router as part of a larger information system, such as a Cable Internet provider? For any given vulnerability there is no one "vendor". The current FAQ leaves many important questions about this process in the air, even assuming you have the legal rights to report something publicly!

In many cases, a company such as Immunity will find vulnerabilities during the course of a commercial penetration test or security assessment. We may not legally be allowed to report these issues ourselves, but our customers may handle that process, or simply want to work around the issue at hand, which they would do by sharing that information with their own teams, possibly with our help. These teams may be international, triggering export rules under the proposed regulation.

To sum up: the current proposed framework for the control of information is unwieldy and unworkable. Information about vulnerabilities needs to be clearly and unambiguously left unregulated by export control to protect the proper functioning of the information security community as a whole.

IMPACT ON VULNERABILITY RESEARCH COMMUNITY

BIS's FAQ states the following would be controlled information.

1. Information "required for" developing, testing, refining, and evaluating "intrusion software", in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information.
2. Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.
3. The development or production of the command and delivery platform itself.

This would be a major sea-change in how the community works. At Immunity, as in other companies in this space, this kind of work is done by a very large team of international individuals, and would require us to cut our US-based-team out of the loop, or apply for thousands of licences a year as we conducted normal research.

There's no way to fix the wording or intent in this area: it simply has to be removed to allow normal functioning of the community and corporate behavior.

SALES

Having to explain to a customer that they have to fill out a form in a language they may not know, and wait up to six weeks to receive an answer is the easiest way to never make any sales ever. Immunity has always had a very reasonable response from the Commerce department, with an average of three weeks for a grant of a licence for our products, based on the existing crypto controls. But imagine if everything you bought from Amazon took an additional three weeks to get back to you as available. Would you continue ordering from Amazon, or would you find another venue to get your products from?

It's for this reason that any arguments that the process is "fine" or fair fall on deaf ears in industry. Anything that slows down sales in this way is not "fine"; it's hugely onerous. Whenever BIS does come back with additional questions, the customers always choose not to buy.

For software, anyone with actual malicious intent can set up a Rackspace account, launch a webpage, and order software from the "US" without the vendor being able to tell the difference between them and a real US company. Immunity goes through great efforts to "know our customers" but there is no easy way to differentiate real from fake in this area.

And yet, in ten years, Immunity has had only one report of our software being used offensively. Whatever threat penetration testing supposedly poses in theory, it simply is not used that way in practice.

POSSIBLE NEGATIVE RESULTS ON US BUSINESSES DUE TO PROPOSED REGULATION

As a matter of routine, practitioners in the information security industry frequently require bespoke tooling to test or demonstrate weaknesses in real-world systems, above and beyond that which any off-the-shelf offering provides. Most often, said tooling is developed by the individual during an engagement and archived in case the work may have relevance, in whole or in part, for clients with similar needs in the future. Initially, this typically takes the form of a single-purpose script or set of commands that are no different than what could be entered manually at a console or debugger, but to do so would sufficiently inflate the cost of these services well beyond that which any corporation attempting to remaining competitive in the market could invest. Tooling of this nature typically does not constitute a commercial-grade product, and may not be in one's interest to broadly distribute under an open source license for ethical, technical, privacy, or economic reasons. This prevents practitioners from easily sharing this work either with fellow practitioners, corporate clients who wish to employ its use in future internal testing (often explicitly requested as a deliverable in the Statement of Work).

To further complicate these matters, these tools are often developed as an extension to, or derivative of, existing software suites that provide value to the industry by enabling these scenarios (Canvas, Impact, Metasploit, Immunity Debugger). While the foundational components provided by the software suite are likely to fall unambiguously into either the export controlled or open source categorization, these extensions or modifications do not, and the licensing structure does not typically allow for redistribution of such work, except in narrow circumstances.

Given that the information security services market is currently underserved, inhibiting these necessary and routine tasks, which have been customary in the industry and in the community for at least two decades, is likely to cause attrition among existing practitioners and discourage new participants from entering the market. This labor shortage, combined with the overhead of legal and regulatory costs for remaining participants, will further apply upward pressure to the cost of security services. This not only impacts the information security industry, but prevents all but the most well-established, high margin businesses from seeking these services. Startups, small and medium businesses, and public services will be overexposed to attacks, and the constraints on entering the information security industry will lead to a deterioration of our technical sophistication relative to that of other nations. Recent large-scale compromises and data loss events (which have both increased in frequency and in impact) have cumulatively caused billions in losses, demonstrating a need to foster growth and development of this industry, not constrain it. As developing nations become increasingly connected to the global marketplace, this need is likely to grow substantially.

STRATEGIC ISSUES

The US has a strategic value in centralizing information security research efforts within the US and within US-owned companies. This allows it unparalleled visibility into the operations and efforts of both allies and competitors. Asking for a license from potential customers has a way of driving these customers to offshore competitors, or incentivizing US companies to partner with

and licence their technology to offshore companies, or simply makes them choose other lines of business to focus on. This reduces American ability to understand and control the global market for information security, attract foreign talent, and maintain our critical lead in cyber security.

SOME IDEAS FOR MAKING THE REGULATION BETTER

Currently, all software that would be controlled under the new cyber regulations is already well controlled under the cryptographic regulations. These regulations offer a licence-free way to sell to all customers in favored countries, and to non government customers in non-favored countries.

At a minimum, the regulation should be rewritten to have the same effect on CANVAS, CORE IMPACT, Metasploit Pro, and similar commercial software as the current regulations allow. This means a broad exception from what the current proposed wording for the new cyber software regulations says. It may be more realistic to only control under this new regulation software which is not purchasable by the public. Any regulation should try to project and predict the sweep of technology moving forward, and have as light a hand as possible on future developments, which will no doubt occur too fast for revisions to take place. Otherwise, the regulation will strangle American innovation in this area, leaving a wide gap for foreign competition to take over.

There is no technical, robust, and long term way to differentiate between the kind of software Hacking Team produces, and the commercial penetration testing market. But additional restrictions could be provided on deals that exceed 1M USD (for the software alone), which may be a way to differentiate specialized deals from normal commercial behavior.

Likewise, any hint of restrictions or controls of vulnerability information should be explicitly allowed, whether “public”, to a “vendor”, or privately held. This area is simply too complex and critical for the export control regulation arena to add value without causing strategic harm.

In addition, very broad exceptions must be written into the regulation to cover normal corporate behavior, including the removal of the deemed export phrasing and the addition of exceptions for inter-corporate transfers. Trying to regulate the transfer of information or software between two co-workers, one of whom happens to have an H1-B, seems insane.

Deep down, software code is not a “weapon” no matter how much the news wants it to be. Penetration testing software and spreadsheets are both useful for companies to accomplish their commercial and compliance goals. What this regulation does in the current proposed form is move commercial gain to overseas companies, without assisting regional stability or human rights efforts in the slightest. The best thing to do would be to remove the language from Wassenaar and if we want to reclassify penetration testing software to better understand it, then simply add an additional classification to it for the reporting piece, since it's all already being controlled via encryption.

Trying to all of a sudden handle export control for the entire vulnerability and penetration testing community in one sudden regulation is like trying to swallow a pineapple all at once. There will be side effects, and they are unfortunately not pretty.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-osux
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0147

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Ansari

General Comment

Hello,

As an information security professional with a long history in working with vulnerability research, security assessment, and defending against threats to systems, networks, applications, and data, I have to express significant concern with the rules proposed here: they are too broad and too restrictive to allow for effective information security practice.

The idea that we can delineate clearly and usefully between tools used for intrusion vs. tools used for security assessment and research is nonsense. Unlike the distinctions between military and civilian use equipment in some categories (a division with less clarity than maybe once before), software development or tools or products can find purpose for both beneficial security defense and as an aid to an attacker or criminal. Attempts to insert an artificial divider and then regulate them will punish legitimate research, allow fewer options for security assessors and defenders to mount an adequate defense, and limit criminals and other malicious actors not at all.

I urge you, along with the many voices in the information security community, to scrap the proposed ruling and collaborate with more and better participants who have the best interests of protecting innocent citizens and organizations from attacks against their information system and data.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-rh5z
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0148

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

It was wise to avoid regulating intrusion software itself, as that would inhibit sharing information and code which was used in an attack, thus preventing victims from warning others (potential victims). This was a brilliant way to handle this issue. Unfortunately, there are still some remaining issues with the regulations, as written.

By controlling "technology" which is specifically designed to develop or use intrusion software, it will have a chilling effect on small businesses in information security. Let me walk through a few examples to illustrate how this makes reporting vulnerabilities to vendors or bug bounty programs require, at least a lawyer who specialized in international trade laws, or at most, filing an application for an export license.

1.) The definition of "technology" includes information. This means that reports which include specific technical data on how a software vulnerability can be exploited would be controlled. This is the information which is critical to developing intrusion software. There is an exception if this information is published to the general public, however this does not allow being discreet in reporting it to just the vendor. While some people feel that it's best to let everyone know about the vulnerability at once (Full Disclosure), there are growing ethical concerns with this as automobiles, surveillance cameras, and medical devices are being connected to computer networks, and often times, the Internet (be it intentional or not). Paying a lawyer to determine if a license is needed is a high enough bar to prevent most people and small companies from ever attempting to report it. When people make these trade offs, they are more likely to err on the

side of caution, so if it's at all possible that they may run afoul of the regulations, they will self-censor out of an abundance of caution.

2.) Often times, vendors will require a proof-of-concept exploit to demonstrate the severity of the issue so they know how to prioritize addressing the issue. With ASLR, DEP, NX, SMEP, and other protection mechanisms, this often needs to be generated dynamically. This software would be very clearly controlled. This is another example of a barrier to people attempting to patch things. While this was clearly not the intent of the regulations in question, it will undoubtedly be the reaction by most law abiding citizens.

3.) It's not clear when a piece of software is foreign or not. For example, in the case of open source software, the code repository may be hosted in the USA, but the majority of the lead developers may be from foreign countries. It's seldom clear what country someone is in based on their e-mail address. Most people agree that the text of the agreement, as written, would require a license before sending any exploit generation "technology" to any foreign country.

To people familiar with international agreement and arms control, it may seem like the line has been clearly drawn, however amongst the information security community, it is confusing legal jargon. Similarly, the lingo of information security is presumably foreign to legal experts. A related issue is the some terms used by computer security experts is imprecise. As a quick example, the term "0-day" could refer to a vulnerability which is not known by either the vendor nor the public, which may be known to vendor but not the public, or that may be known by everybody but no patch has been released by the vendor.

The question of how to modify the regulations to mitigate these problems remains an open one. Clearly, making exceptions isn't going to be effective since then new technologies may be inadvertently regulated until an exception could be made for them. On the other hand they may not be regulated, thus allowing criminals a loophole until the regulations can be updated.

One option would be to regulate the payloads of intrusion software, rather than the tools to make the intrusion software itself. A proof-of-concept will typically include "popping a shell," which allows running arbitrary commands on a compromised computer, and they often include the ability execute arbitrary machine code. However, if the regulations targeted the software which steals passwords, encryption keys, and so forth, this might offer a path forward. Great care would have to be taken to prevent the control of backup software. It is conceivable that administrators would want to access all the machines on their network and ensure that they are properly backed up. We would not want to regulate this type of activity.

I hope that the regulations will be updated to address the concerns of the community of people who will be directly affected by these rules, and that there be a comment period for the updated text.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-1qic
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0149

Comment on FR Doc # 2015-11642

Submitter Information

Name: Robert Radvanovsky

General Comment

As a cybersecurity professional and researcher, I am concerned about the legal, political, and economical implications that this would have on the United States. Furthermore, I would be concerned about violating the Bill of Rights for the United States, specifically the First (Right of Free Speech) and Second (Right to Bear Arms and Munitions) Amendments. As encryption was previously classified as a "munition" by EAR, this would contradict the Second Amendment.

On an international basis, this would conflict with both national and international businesses being capable of performing business transactions, storage of critical documentation, limit cloud computing capabilities, and force massive bureaucratic rules and regulations on the daily use of encryption as well as any security application, device or software thereof, in an effort to secure both data in-transit as well as data at-rest.

From a practical perspective, the only parties impacted are honest everyday citizens, while criminal activities will not only continue, but perhaps increase in intensity.

From an economic perspective, this may cause cybersecurity businesses, research and academic organizations to move outside of the United States.

Overall, imposing such limitations would stifle innovation, creative works, et. al within the United States, and perhaps, abroad.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-swmr
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0150

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Osborn

Address:

Goodwin Procter LLP
901 New York Avenue NW
Washington DC, DC, 20001

Email: josborn@goodwinprocter.com

Phone: 202-346-4133

Fax: 202-346-4444

Organization: Core Security

General Comment

See attached file(s)

Attachments

Core Security's comments to BIS's proposed rule - FINAL



Core Security’s Comments to “Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items,” 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63.

Core Security Technologies, Inc. (“Core Security”), a Delaware corporation that develops and sells security-testing software and provides related security services, submits these comments to the rule proposed by the Bureau of Industry and Security (“BIS”) involving the control of intrusion-delivery software. *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 97 (proposed May 20, 2015), pp. 28853-63 (“Proposed Rule”). Core Security strongly opposes the Proposed Rule and believes its promulgation without significant amendments would provoke consequences that are unintended and ultimately detrimental to the U.S. national security and to the viability of the U.S. penetration-testing industry.

In Part I below, Core Security introduces its business and the software and services relied upon by its customers for network and system security. In Part II, Core Security explains why it believes the Proposed Rule would: (i) cripple Core Security’s business and other U.S. businesses operating in the security space that are above-board corporations seeking to comply with U.S. regulations; (ii) have a detrimental effect on cybersecurity and preventing cyberattacks worldwide; and (iii) be ineffective as a means to thwart malicious actors — including human-rights abuses abroad — who use intrusion software for offensive and malicious purposes. In Part III, Core Security recommends modifications to the Proposed Rule that would alleviate the concerns expressed in Part II. And, in Part IV, Core Security provides responses to the specific questions posed by BIS. *See* Proposed Rule at 28,856.



I. Core Security’s Business and Offerings

Core Security provides cyber-security solutions that are used to protect its customers’ networks and systems. Founded in 1996 in Buenos Aires, Argentina, and now co-headquartered in Boston, MA and Buenos Aires, Core Security has since grown to approximately 150 employees. Core Security has a long history of working very closely and cooperatively with BIS’s Information Technology Controls Division to ensure its compliance with the EAR.

To help its customers protect their networks and digital assets, Core Security provides penetration-testing software, including its flagship product, Core Impact Pro®. Core Impact Pro enables comprehensive, real-world security testing on customer networks by performing a penetration test of a network to identify, analyze, exploit, and document security vulnerabilities. The penetration test is executed from a console, typically installed on a laptop or other computer, that installs agents in target hosts. Installed agents, in turn, can install additional agents in the target network to further conduct a penetration test. The penetration test gathers information about the target host, runs exploit modules against publicly known vulnerabilities, and simulates attacks against the target network and system to determine weaknesses. Core Impact Pro includes a security-testing feature for wireless networks, mobile devices, a password cracker for “brute forcing” stored passwords, and a fake access-point software module used with third-party hardware to test WiFi weaknesses.

A second software product provided by Core Security is Core Insight®, an automated security-testing and risk-assessment solution that allows continuous network assessment and includes some of the same capabilities as Core Impact Pro. Core Insight reveals paths of exposure in web applications, networks, and client-side weaknesses, producing metrics to validate security controls and address data-breach threats. The Core Insight security test is executed by automated software running on an appliance that simulates and then optionally attempts the installation of agents in target hosts using security vulnerabilities. Similar to Core Impact Pro, the installed agents can in turn install additional agents in the target network to



further test security vulnerabilities and target the information and systems the user is attempting to test.

Core Security also offers product training services, consulting services, technology and security research, and open-source tools for the IT community. Training services can be provided remotely or at the client site. Core Security’s software is designed to be used by a trained IT professional: the easy-to-use and intuitive user interface and console, along with on-demand training, sets Core Security’s offerings apart from its competitors. Core Security’s training services generally involve the provision of technology about how to use the Core Security software, as well as specific guidance on how to use the software to test the client’s unique network, applications, and systems. Core Security also partners with third-party training partners (*e.g.*, InfoSec Institute, Axxum Technologies, and the Hacker Academy) that offer academic instruction and have special expertise with Core Security’s software.

Core Security provides consulting services, ranging from comprehensive penetration tests to simple web-services assessments, wireless-penetration tests, application-penetration tests, and source-code audits. Core Security delivers a variety of consulting services in order to provide its customers with the broadest range of defensive assessment capabilities.

Core Security performs security research for the IT community. In 1997, Core Security established the CoreLabs Information Security Research group. “CoreLabs” anticipates future needs and requirements for information-security technologies. CoreLabs publishes a research blog, vulnerabilities, and advisories, and develops new exploits and open-source tools for the IT community. Core Security also provides a suite of open-source tools developed by CoreLabs for the benefit of the IT security community.¹

Core Security’s spectrum of software products and services draws customers from various industries — domestic and foreign — including:

¹ These tools provide various functionalities, and are made publicly available at the URL <http://www.coresecurity.com/grid/index-open-source-tools>.



- Public and Private Universities – Fordham, Harvard, Texas Tech, and Penn State Universities.
- Utilities and Energy – Chevron, Southern Cal Edison, Long Island Power, National Grid UK, Natural Resources of Canada, Emirates Nuclear Energy, Qatar Petroleum, Philippine Long Distance Telephone, and Honeywell.
- Financial services – Bank of New York Mellon, Capital One, Citi group, T.Rowe Price, Charles Schwab, Commercial Bank of Ethiopia, Banca d'Italia, National Bank of Canada, and BDC Canada.
- Government – US Department of Energy, US Department of State, US Department of Treasury, US Army/Navy/Marines, US Homeland Security, Carabineros de Chile, Korea National Police Agency, Canadian Department of National Defense, Abu Dhabi General Secretariat, and City of Houston (Utilities/Police/Airport).
- Healthcare, pharmaceutical, and insurance firms – Quest Diagnostics, Blue Cross, Kaiser, and Green Shield Canada.
- Major manufacturers – Cargill, Black & Decker, Thermo Fisher, Hyundai, Honeywell, and Bridgestone.
- Media, entertainment and travel companies – Fox, McDonalds, Disney, and United Airlines.
- Major retailers – Home Depot, Nestle, Costco, PetSmart, Target, and Starbucks.
- Security consulting firms – Raytheon, PricewaterhouseCoopers, Booz Allen Hamilton, and Deloitte, Hewlett Packard, and IBM Internet Security Systems.
- Technology firms – Cisco, Lenovo, Microsoft, MacAfee, and Symantec.



- Telecommunications firms – Verizon, Bell Mobility, Telefonica, China Mobile, and British Telecom.

II. Negative Impact of The Proposed Rule

For Core Security’s customers, the security needs addressed by our products and services are both critical and incessant. Daily news headlines depict public and private sector actors under constant cyberattack. On July 9, 2015, the federal government announced that 22 million people were affected by cyberattacks on the Office of Personnel Management, leading to loss of social security numbers and other personal, financial information.² The cyberattack on OPM was reportedly linked to the Chinese government. On the commercial side, Home Depot, the world’s largest home improvement retailer, announced in November of 2014 that credit card and personal data for some 53 million users were stolen during a breach.³ According to Home Depot, the breach involved the use of custom-built malware installed on Home Depot’s self-checkout systems. *Id.* These are but two recent examples of many.

The offensive use of intrusion-delivery software also raises human-rights concerns. For example, Egyptian dissidents who ransacked the offices of Egypt’s secret police following the overthrow of Egyptian President Hosni Mubarak discovered a contract with a third-party to use the FinFisher spyware software to spy on Egyptian citizens and political adversaries.⁴ As another example, in 2014 an American citizen alleged the Ethiopian government had surreptitiously downloaded FinFisher on his computer and was using the spyware to wiretap his

² Nakashima, Ellen, “Hacks of OPM databases comprised 22.1 million people, federal authorities say,” *The Washington Post* (Jul. 9, 2015).

³ Press Release, The Home Depot, “The Home Depot Reports Findings in Payment Data Breach Investigation,” (Nov. 6, 2014).

⁴ Leyden, John, “UK firm denies supplying spyware to Murbark’s secret police,” *The Register* (Sept. 21, 2011).



private Skype calls and monitoring his family’s use of the computer over the period of a few months.⁵

For these and other reasons, the government, public, and business communities in the United States and among our global friends and allies have a shared interest in ensuring that malicious software is not obtained by malicious actors or used maliciously — indeed, never has the need for protection against these sorts of cyber intrusions been more acute than it is today. But this is precisely why it is vital to maintain and encourage U.S. dominance in this space, and to ensure that products, services, and technology, such as those offered by Core Security, are available for *defensive* use in protecting enterprises, government, and individuals. The Proposed Rule threatens to cripple this industry in the United States, driving it offshore and, ultimately, outside of the reach of U.S. jurisdiction and regulation, as we now explain.

A. The Proposed Rule Would Cripple Core Security and Other U.S. Businesses

Core Security’s software and technology would appear to meet the criteria of 4D004 as software (and related technology) specially designed or modified for the generation, operation or delivery of, or communication with, intrusion software (*i.e.*, “intrusion-delivery software”). As explained by the Proposed Rule, Regional Stability (“RS”) controls would apply to intrusion-delivery software and technology and would require a validated license for export to all foreign countries other than Canada. The Proposed Rule would eliminate Core Impact Pro’s eligibility for License Exception ENC — indeed, other than a limited GOV license exception for exports to U.S. government entities abroad, there would be no license exception available for this product. And, most harmful to Core Security, the Proposed Rule would create a presumption of denial for licenses to export intrusion-delivery software and technology that has or supports “zero-day” exploits and “rootkit” capabilities, as Core Security’s products appear to do (which we address more fully in Part III below).

⁵ Cardozo, Nate and Cohn, Cindy, “American Sues Ethiopian Government for Spyware Infection,” Electronic Frontier Foundation (Feb. 18, 2014).



The proposed presumption of denial threatens to eliminate the roughly 20% of Core Security’s sales that are made outside of the United States. This includes sales to the foreign branch offices and foreign subsidiaries of iconic U.S. companies; to NATO allies; and to multinational companies whose networks house data belonging to U.S. companies or the protection of which is otherwise vital to the U.S. national security. So it is baffling to Core Security and to many others submitting comments that, in the name of denying offensive tools to bad actors intent on doing harm to the United States, the Proposed Rule would deny to these and other legitimate organizations the critical tools necessary to defend themselves against cyberattacks.

The Proposed Rule would create internal software development impediments for Core Security, limiting our ability to employ or engage non-U.S. citizens, since it would require us to apply for “deemed export” licenses — again under a policy of presumptive denial. Thus, predictably, the U.S. domestic development of defensive cybersecurity tools will fall behind, as foreign talent in this space will become harder or perhaps impossible to enlist. These limitations will strike especially hard at Core Security, whose non-U.S. person workforce is roughly 58% of its total, with the majority of software development conducted in Argentina. Given the ambiguous demarcation between controlled and non-controlled technology (even under the most painstakingly worded regulations in the EAR), it could be impractical and perhaps impossible to cabin its non-U.S. workforce to only non-controlled software and technology. Thus, even as we face a proliferation of threats from abroad, we will become an inward-looking domestic industry. We will lose our effectiveness, to the ultimate detriment of the U.S. national security and industrial base.

Many other U.S. businesses are likely to be similarly affected and competitively disadvantaged vis-à-vis security firms providing non-U.S. origin software and technology. Even for products not incorporating zero-day exploits or rootkit capabilities, the administrative burdens, cost, and delay involved in seeking licenses for foreign customers would be detrimental to U.S. industry. Significant time, costs, and legal fees would be required to understand and

comply with the license application process for each foreign customer and employee. Time is of the essence in emergency data-breach situations. The delay between when a penetration-testing product is needed and when a BIS export license is authorized can decide a customer's fate.

Another obvious consequence of the Proposed Rule is to hand to non-U.S. producers of intrusion-delivery software a critical and perhaps decisive distribution advantage over U.S. firms. Although each signatory to the Wassenaar Arrangement has committed to controlling intrusion software, none appears to have adopted anything approaching the level of restriction in the Proposed Rule. For instance, the European Union has implemented minimal controls to intrusion-delivery software by adding the item to Annex I to Regulation (EC) No. 428/2009.⁶ Except for a subset of Annex I items designated for stricter controls and listed in Annex IV, the transfer of items within the EU community requires only that exporters maintain records for at least three years, and indicate on commercial documents that the items are subject to further controls if exported from the EU community.⁷ The vast majority of Annex I items, including intrusion-delivery software, may be traded freely — without registration or licensing — within the EU community.⁸ Exports from EU Member States to seven “friendly countries” — Australia, Canada, New Zealand, Japan, Norway, Switzerland, and the United States — are only slightly more encumbered: any EU Member State exporter may use EU General Export Authorization number 001(EU GEA 001) to send Annex I goods to one of the friendly countries, by simply notifying the Member State from which they are exporting within 30 days after their first export.⁹ EU Member States may require exporters to register prior to using EU GEA 001,

⁶ See Commission Delegated Regulation 1382/2014, at 13, 130-31, http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_152996.pdf.

⁷ See Council Regulation 428/2009, Annex IV, pp.260-66, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF>. Annex IV includes military, cryptologic, and chemical-weapons related items that are subject to additional restrictions, even when transferred within the EU community. See also Council Regulation 428/2009, Ch. VIII, art. 22(1), p.9; Ch. VIII, art. 22(8) p.10; Ch. VIII art. 22(10), p.10.

⁸ See *The EU Dual Use Export Control Regime*, European Commission, at 2 (Feb. 2, 2014), http://trade.ec.europa.eu/doclib/docs/2014/february/tradoc_152181.pdf.

⁹ See *id.* at 254.



but such registration “shall be automatic and acknowledged by the competent authorities to the exporter without delay and in any case within ten working days of receipt.”¹⁰ For most (if not all) of the Member States, this additional requirement is a simple, one-time pre-registration process.¹¹ Under the Proposed Rule, meanwhile, U.S. exporters will plead for their would-be customers’ patience as they await issuance of BIS licenses — unless, of course, the needed products confront a presumption of denial that could effectively bar export altogether.

In sum, the Proposed Rule will be damaging for Core Security and for the U.S. cybersecurity industry by creating an uneven international playing field.

B. The Proposed Rule Would Undermine the Prevention of Cybersecurity Attacks Worldwide

The Proposed Rule will hinder the defensive cybersecurity efforts of U.S. and non-U.S. entities with foreign locations. Perhaps most problematic is that the Proposed Rule eliminates the license exception for exports to certain private sector end-users wherever located that are headquartered in a country listed in Supplement No. 3 to Part 740 of the EAR, subsidiaries of U.S. corporations, or to employees or contractors of U.S. firms at 15 C.F.R. § 740.17 that has served long and well the scores of U.S. companies that make and export encryption functionality software.

And because the need for security software and technology often arises immediately (e.g., in an emergency breach situation), when delay occasioned by a license application

¹⁰ *See id.*

¹¹ *See, e.g., Open General Licences: An Overview*, UK Export Control Organisation (Aug. 23, 2012), <https://www.gov.uk/open-general-licences-an-overview>; *Brief Outline on Export Controls*, The Federal Office of Economics and Export Control, at 11 (2013), http://www.bafa.de/bafa/en/export_control/publications/export_control_brief_outline.pdf; *User Guide on Strategic Goods and Services for The Netherlands*, Ministry of Foreign Affairs, at 30 (2013), available at <http://www.government.nl/issues/export-controls-of-strategic-goods/documents-and-publications/directives/2012/04/12/user-guide-on-strategic-goods-and-services.html>.



requirement can be fatal to a cyberdefense objective, the Proposed Rule will render non-U.S. entities — including the many foreign subsidiaries of U.S. companies that Core Security counts among its customer base — more susceptible to damage from cyberattacks. Indeed, the Proposed Rule may diminish even the security of U.S. companies at home as oftentimes a vulnerability at a foreign subsidiary can provide an attack vector into domestic networks and systems.

Although U.S. subsidiaries might more easily source penetration-testing products from abroad, these products may not be as effective as those provided by U.S. firms, and U.S. subsidiaries may lack the familiarity and experience with foreign-sourced products that they would have with U.S.-origin products and services.

The unavailability of a license exception for deemed exports of controlled software and technology to employees or contractors of U.S. firms would also add an administrative burden and additional layer of diligence to the process of providing software and technology to even household-named U.S. firms.

These anticipated casualties of the Proposed Rule seem far too high a price to pay for discharging U.S. commitments under the Wassenaar Arrangement, and especially in light of how other member countries are satisfying their equivalent commitments.

C. The Proposed Rule Would Be Ineffective to Thwart Malicious Actors

The damaging effects of the Proposed Rule are abundant, yet its promised benefits are difficult to perceive. To begin, the Proposed Rule does not address the delivery of offensive exploits within the United States and utilizing entirely domestic tools. And the Proposed Rule does not control or even address the vast majority of situations involving the delivery of harmful software, malware, and spyware. In most cases of malicious intent, Core Security believes that an actor will develop a harmful exploit, test the harmful exploit, deliver the harmful exploit, and then maliciously attack a network or system without in any way utilizing software or technology affected by the Proposed Rule. As one such example, assume that a malicious actor creates an



exploit based on an SQL injection (*i.e.*, malicious SQL statements inserted into an entry point for execution). The exploit itself, a string of SQL code, will not be controlled by the Proposed Rule because the Proposed Rule does not control exploits. Now assume the malicious actor delivers the SQL injection to the target using standard HTTP. Because HTTP (and the components required to invoke HTTP) is not specially designed or modified for the “generation, operation or delivery of, or communication with, intrusion software,” it would not be controlled by the Proposed Rule. Additionally, assume that the command and control used to read and write to the network connection is Netcat, a common and publicly available open-source tool. Here again, because Netcat is open-source and freely and publicly available, it also would not be controlled by the Proposed Rule. Even if the SQL injection represented a zero-day exploit, nothing described in the above scenario would appear to trigger the restrictions in the Proposed Rule.

To take an example that is real and current, the internal corporate records of Italian-based Hacking Team were compromised and over 400GB of its data were leaked to the Internet.¹² This exposed the Hacking Team as a provider of its intrusion-delivery platform — capable of serious misuse in the hands of governments conducting surveillance on their citizens — to governments involved in mass genocide such as in Sudan. *Id.* At this point it remains unclear whether the Italian-based Hacking Team and the apparent provision of software and services to Sudan were even subject to U.S. jurisdiction, so it remains unclear whether the Proposed Rule would have had *any* affect over Hacking Team’s unscrupulous provision of assistance to the Sudanese government. But even if those activities were subject to U.S. jurisdiction, the supply of software to the Sudanese government was already unlawful under the EAR and U.S. economic sanctions against Sudan. To suggest that the addition of the restrictions in the Proposed Rule would prevent these sorts of occurrences simply rings hollow, yet the cost of adding the restrictions is undeniable.

¹² Valentino-Devries, Jennifer and Yadron, Danny, “Hacking Team, the Surveillance Tech Firm, Gets Hacked,” *The Wall Street Journal* (Jul. 6, 2015) (available at <http://www.wsj.com/articles/hacking-software-maker-gets-hacked-1436223757>).



Indeed, most malicious cyberattacks will not be affected at all by the Proposed Rule — and particularly because tools widely used for generating, delivering, or controlling exploits are open-source and freely available, or else not otherwise subject to U.S. jurisdiction, and so could not be affected by the Proposed Rule. *See* 15 C.F.R. § 734.3(b)(3). These open-source, freely available tools are far more likely to be called upon by actors intent on perpetrating malicious cyberattacks than are the legitimate, professional penetration-testing products offered by Core Security and its competitors. In its nearly 20-year history, Core Security has only been made aware of a single instance in which Core Security’s software has been allegedly used for malicious, offensive purposes.¹³ And even this single instance remains uncorroborated and unconfirmed. Yet Core Security’s software has been used for legitimate defensive purposes hundreds of thousands of times.

III. Proposed Modifications to the Proposed Rule

A fundamental problem with the Proposed Rule is that it too restrictively controls a broadly defined category of intrusion-delivery software and technology that is fundamental to protecting global networks and systems. In an effort to pare back the Proposed Rule’s broad, counterproductive effects, we offer the following suggestions.

A. Current Export Controls Are Adequate

As a first suggestion, we would ask BIS to reconsider implementing the Wassenaar Arrangement under the existing provisions of License Exception ENC, which are likely to apply to most or possibly all affected forms of intrusion software.

Based on years of experience working under the encryption-controls regulations, we think the current regime adequately and effectively balances the global need to secure networks and systems with the compelling interest of making it difficult for malicious software to be obtained by malicious actors or used maliciously. Under the current regime, Core Security

¹³ *See* <http://www.reuters.com/article/2014/12/27/us-hacking-tool-idUSKBN0K50HI20141227>.



provides detailed, product-specific Classification Requests to BIS. Core Security is required to provide BIS with semi-annual reports detailing all exports of its software. And for foreign government end-users, Core Security is required to obtain a license before exporting its software or technology. These are not ministerial filings met with a rubber stamp, as BIS has denied at least six license applications based on concerns that the Core Security software may be used by a foreign government for wrongful, offensive purposes.

If, against this experience, the U.S. government has evidence that the current regime for regulating this type of software has proven ineffective, we would ask that the evidence be made public so that affected members of industry may play a constructive role in narrowly tailoring new regulation to counter the actual deficiencies. At the very least, Core Security invites BIS to propose modified rules and provide a comment period so that affected members of industry have an opportunity to provide constructive feedback.

B. Control Only Those Tools With No Legitimate Uses

If BIS is determined to remove the eligibility of License Exception ENC for intrusion-delivery software, then the rule should be made to apply to those tools for which there are no apparent, legitimate defensive uses.

Just as the Proposed Rule has brought together competitors and collaborators to discuss how best to discharge the United States' Wassenaar Arrangement obligations, we think it would be a grave and costly mistake to conclude, without substantial effort, that BIS, working hand-in-hand with affected industry members, could not draft a rule that distinguishes these malicious software products from legitimate cybersecurity solutions of the sort that Core Security provides to customers worldwide. For instance, BIS is already able to review the materials submitted in support of a Classification Request to determine whether the software under review has legitimate non-malicious purposes. BIS could further require an exporter to provide details about why and how a given item has legitimate, non-malicious purposes or a predominantly defensive intention. In that way, malware-delivery, spyware-delivery, and malicious exploits-



delivery products having only nefarious purposes could be appropriately restricted in their distribution, leaving legitimate products such as Core Impact free of restrictions that could eliminate its foreign distribution altogether.

BIS could also rely more substantially on written end-use statements committing end-users to uses of the software on their owned and controlled networks, software, systems, and hardware, and committing such end-users to audits or visits by BIS agents to test compliance. And BIS could enforce significant civil and criminal penalties against an end-user for violation of this end-use statement. This would bring the regulation of intrusion software in line with other laws and regulations (*e.g.*, Computer Fraud and Abuse Act and the Electronic Communications Privacy Act) whose proscriptions turn on specific conduct and intent rather than the technical characteristics of an item such as Core Impact Pro, on which scores of legitimate companies and government entities rely to protect their networks.

C. Define “Zero-Day” Exploits As Those Exploits Which Are Unpublished And Unknown To the Target Software’s Vendor

For Core Security, perhaps the most troublesome aspect of the Proposed Rule is that it would create a presumption of denial for applications to export tools supporting the delivery of “zero-day” exploits. We are concerned that BIS has misapprehended the nature of software that supports zero-day exploits, causing it to wrongly conclude that such software is necessarily malicious and that its exportation would rarely if ever serve legitimate ends. As explained below, Core Security may unwittingly have contributed to this misapprehension through comments made to BIS in connection with an appeal of BIS’s denial of certain license applications.

Core Security understands BIS to define zero-day exploits as exploits for which a patch is not yet available. A better definition, we think, would be: *exploits that are unpublished and unknown to the target software’s vendor*. This definition would better capture what BIS intends from the Proposed Rule, as it would save from the policy of denial a product like Core Impact,



which is *not* specially designed to support exploits that are unpublished and unknown to the target software's vendor. Core Impact has tremendous *defensive* utility because it helps a customer identify exploits for which a patch is not yet available, enabling critical remedial measures (other than via a patch) to protect against such exploits. For example, companies wishing to secure their own systems against a vulnerability may require testing using the zero-day exploit in order to make the difficult decision to take a machine offline or create air gap or other barriers to reaching the affected machines. Another legitimate technique is to test one's system against an exploit that does not yet have a released patch to see if the defensive cybertools utilized by the target are able to identify that an attack is occurring (this is called looking for signatures). Even if a patch is not yet available for an exploit, the exploit may well be useful for ensuring that one's system is able to identify when that exploit is being advanced, since this critical information can prompt protective counteraction.

On the other hand, exploits that are unpublished and unknown to the vendor are much more likely to be utilized for malicious purposes. When a white hat (*i.e.*, ethical, nonmalicious) security researcher discovers an exploit in an application or system, the researcher has a strong interest in notifying the vendor about the vulnerability so that it can be promptly patched. One such platform for making these vulnerabilities publicly known is the Common Vulnerabilities and Exposures system.¹⁴ But when a black hat security researcher (one who violates computer security with malicious intent or for personal gain) discovers an exploit in an application or system, the researcher has an interest in *not* notifying the vendor about the vulnerability so that he can take advantage of the exploit. As a real-world example, the recent Hacking Team breach resulted in the discovery of various exploits (*e.g.*, critical vulnerabilities in the Adobe software) that were not made previously known to Adobe or otherwise published. The delivery of this type of vulnerability, unknown to the vendor and otherwise unpublished, is far more likely to be utilized for offensive or malicious purposes.

¹⁴ See <https://cve.mitre.org/>.



Core Security does not provide its customers with exploits (or testing support) for testing vulnerabilities that are unpublished or unknown to the vendor. CoreLabs actively publishes the vulnerabilities that it discovers, and notifies the target vendors, when possible. This is the most effective way to ensure that the public understands vulnerabilities and their risks and that a patch or fix is created as soon as possible, while other measures are taken in the interim.

D. The Presumptive Denial Should Be Limited to Tools “Specially Designed” to Support Rootkits or Zero-Day Exploits

Core Security is also very concerned that the Proposed Rule would create “ a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.” Proposed Rule at 28,858.

Many intrusion-delivery tools, such as those offered by Core Security, include functionality for inserting custom exploits or rootkits. Similar to zero-day exploits under Core Security’s proposed definition, support for rootkits also may have legitimate, non-malicious purposes, such as testing one’s own network and systems to ensure that a system is able to properly identify the rootkits’ signature. And this functionality is necessary for Core Security’s customers to test exploits and rootkits specific to their applications, networks, and systems. Accordingly, if a presumptive export license denial is appropriate for *any* item, it should be limited to those items that are “specially designed” to support rootkit or zero-day exploits. As Core Security previously explained to BIS in a presentation, the Core Security products do not *include* rootkits (or zero-day exploits under Core Security’s definition of that term), although the products could be used to deliver such items. This modification to the Proposed Rule’s licensing policy could help to ensure that a presumptive denial does not inadvertently swallow the numerous products that support flexibility for testing against vulnerabilities specific to a customer’s network and systems.



E. License Exceptions for Exports to U.S. Subsidiaries, Developers, and Contractors for Internal Company Use

Some of the most important, widely used license exceptions available for the export of encryption items authorize exports to U.S. subsidiaries abroad, private-sector end-users wherever located that are headquartered in a country listed in Supplement No. 3 to Part 740 of the EAR, businesses located abroad but headquartered in the United States, and foreign developers and contractors of a U.S. company, as specified in 15 C.F.R. § 740.17(a). It is hard to understand the rationale for a wholesale elimination of these types of license exceptions in the Proposed Rule, since the encryption regulations have long operated on precisely this basis, without apparent detriment to the national security and with a diminished regulatory burden on BIS. Indeed, hundreds of legitimate private and public sector businesses rely “24-7” on Core Security’s products and services (as the illustrative examples in Part I above show), yet many of these entities, and/or their foreign branches and subsidiaries, would be suddenly denied protection under the Proposed Rule.

And the unavailability of the important license exceptions for deemed exports of controlled software and technology to employees or contractors of U.S. corporations would unnecessarily retard the advancement of security technology and research and development for U.S. corporations. We predict and fear a drain of technical talent as a result of the Proposed Rule.

F. License Exceptions for Exports to the EU and Friendly Countries

The effectiveness of a multi-lateral export control regime such as the Wassenaar Arrangement depends not only on the signatories agreeing to specific language defining the technical categories of items on the Commerce Control List, but also and more importantly on similar licensing and control practices amongst the signatories. As explained, however, the EU has *not* implemented Draconian controls such as those outlined in the Proposed Rules has instead authorized the free flow of intrusion software among and between EU countries, and even to



countries outside of the EU, including the United States. BIS should at a minimum implement license exceptions authorizing export to friendly countries such as the EU Member States and other Wassenaar signatories. Absent such parity of treatment, it is hard to see why any company in this space would remain in the United States, where the proposed barriers to export and research/development work are so high.

G. Clarification of Controlled Technology

Core Security believes that the Proposed Rule fails to help the regulated public identify what “technology” would be controlled. Without a clear articulation of these important concepts, the level of actual compliance with the rule that is finally implemented is almost certain to be low.

An important part of Core Security’s business is training its customers on how to use the Core Security software and technology in order to conduct penetration testing to protect the customers’ networks and systems. Core Security trains its customers on how to install and use its software, including how to develop testing specific to the customers’ network and systems. Because the Core Security software provides functionality for the customer to create and insert custom exploits, would training on how to use this functionality be considered controlled technology regarding the “development or production of the command delivery platform itself,” or “information on how to prepare the exploit for delivery or integrate it into a command and delivery platform”?¹⁵ Or, would it instead be considered decontrolled “information ‘required for’ developing, testing, refining, and evaluating ‘intrusion software’”?¹⁶ Arguably, this type of technical training meets both criteria, leaving Core Security without clear guidance for how to deal with its non-U.S. customer base.

Core Security believes that the ambiguity in the definitions and control of “technology” would create an unworkable regulatory regime.

¹⁵ See BIS FAQ #4, available at <http://www.bis.doc.gov/index.php/policy-guidance/faqs>.

¹⁶ *Id.*



IV. Core Security’s Responses to Questions Posed By the Proposed Rule

- 1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:**

Core Security estimates that it would be required to submit approximately 310 license applications per year under the requirements of the proposed rule.

- a. How many additional applications would be for products that are currently eligible for license exceptions?**

Core Security estimates that it would be required to submit approximately 150 license applications per year under the Proposed Rule for products that are currently eligible for license exceptions.

- b. How many additional applications would be for products that currently are classified EAR99?**

Core Security does not believe that it would be required to submit any additional license applications under the Proposed Rule for products that are classified as EAR99.

- 2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?**

Core Security estimates that it would be required to submit approximately 160 deemed export license applications per year under the requirements of the Proposed Rule.



3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company’s ability to protect your own or your client’s networks? If so, explain how.

Yes, for all of the reasons provided above, the Proposed Rule would have negative effects on Core Security’s legitimate vulnerability research, audits, testing and screening, as well as Core Security’s ability to protect its own and its clients networks.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? If this information you already have for your products?

Core Security estimates that it would take approximately forty (40) hours to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748. In the ordinary course of its business, Core Security does not maintain the information organized in the manner requested by the supplement.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-like
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0151

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

Organization: Rapid7, Inc.

General Comment

Please see attached.

Attachments

Rapid7 - Comments to FR Doc #2015-11642



Rapid7 Comments for the Bureau of Industry and Security's Proposed Rule Implementing the Wassenaar Arrangement 2013 Plenary Agreements Regarding Intrusion and Surveillance Items

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Avenue, N.W.
Room 2099B
Washington, D.C. 20230

RE: Comments of Rapid7, Inc. Regarding the Bureau of Industry and Security's Proposed Rule Implementing the Wassenaar Arrangement 2013 Plenary Agreements Regarding Intrusion and Surveillance Items (80 Fed. Reg. 28853, May 20, 2015)

Ref: RIN 0694-AG49

Dear Sir/Madame:

Rapid7, Inc. ("Rapid7" or the "Company") submits these remarks in response to the request from the Bureau of Industry and Security ("BIS") for comments regarding the proposed rule implementing the agreements reached during the Wassenaar Arrangement's 2013 Plenary meeting (hereinafter the "Proposed Rule").

We appreciate the opportunity afforded by BIS to review the Proposed Rule and to provide comments prior to its implementation. As explained in more detail below, as a custodian and exporter of a security testing platform that would be subject to restrictive licensing requirements under the Proposed Rule, we are deeply concerned that the ultimate impact of the Proposed Rule would be to undermine (rather than enhance) cybersecurity. Specifically, we believe that the Proposed Rule would have a chilling effect on cybersecurity-related research and development efforts and make it harder for security professionals to access and deploy cutting edge tools within their organizations. Over time, we believe that the cumulative impact of the proposed controls would be to erode the effectiveness of security testing products and to impede their legitimate use. We urge BIS to reconsider the Proposed Rule in light of our comments below, and the comments provided by other interested parties. Due to the significant potential impact of the Proposed Rule on a vital part of the cybersecurity industry, we respectfully request that BIS issue another round of proposed controls before implementing a final rule.

Background

Security professionals depend on a mix of open source and commercial tools to assess their organization's security and to identify and mitigate vulnerabilities before an attack can occur. In order to be effective, these tools must mimic the tactics and capabilities of would-be attackers, including the execution of known exploits; circumvention of anti-virus and firewall; and use of the precise techniques that real attacks use to break passwords and exfiltrate data. Although some of these tools can be considered intrusion software, they are designed with the goal of improving security. In fact, certain regulated organizations are affirmatively required



to conduct periodic penetration testing using these tools to ensure that they are protected against attack.¹

Rapid7's cybersecurity data and analytics software and services help organizations reduce the risk of security breaches, detect and respond to attacks, and build effective cybersecurity programs. Security begins with identifying all network vulnerabilities that expose organizations to attack, and systematically reducing that exposure. Rapid7's Metasploit products and similar security testing solutions help organizations identify weak points in their IT environment, understand the potential impact of an attack, and mitigate the threat. Such mitigation may include deployment a patch if one is available, removing IT assets from a network, or separating databases from other parts of the network to make it harder for attackers to reach them. In instances where patches are not available, identifying and implementing alternative measures becomes even more critical.

The open source Metasploit Framework is a leading penetration testing platform that was downloaded over 200,000 times in 2014 by users across a range of industries and geographies. This technology is developed in conjunction with the wider information security community and is a critical component of many security toolkits. Rapid7 is the custodian of the Framework and employs a dedicated team of engineers who vet contributions to the Framework to ensure that such contributions do not include back-doors or other mechanisms that could make a user of the Framework vulnerable to an attack.

Rapid7 develops proprietary software based on the open source Metasploit Framework. This software includes the same attacks as the open source code, but provides additional value through automation, integration, reporting, and ease-of-use. The flagship product, Metasploit Pro, is used by security consultants and cybersecurity teams to perform security audits and penetration tests. The intrusion functionality provided by Rapid7's proprietary software is identical to the capabilities of the open source framework, which is available to the public through GitHub.com and similar distribution points for open source products.

The Proposed Rule would greatly increase the licensing burden on proprietary versions of Metasploit

Rapid7 receives hundreds of inquiries daily from individuals and entities outside the United States seeking to either purchase a Metasploit product, or to access a free or trial version of the software.

Proprietary versions of Metasploit are subject to export restrictions under the Export Administration Regulations ("EAR") and currently require a specific license for export to government end-users outside the United States and Canada. Rapid7 personnel manually screen all incoming product requests to determine whether an export license is required. Currently, Rapid7 submits approximately 10 export license applications per week to BIS. Under the Proposed Rule, Rapid7 would have to apply for licenses for all Metasploit exports, not only exports to government end-users. As a result, Rapid7 anticipates that the number of license applications would increase ten-fold to approximately 100 export license applications per week. Such an increase would require a significant investment by the Company to prepare the license applications, make further growth of the commercial product virtually impossible, and ultimately result in individuals, companies and agencies being less safe from attack.

The cost of these efforts would ultimately be reflected in the price of Rapid7's products, thus making them less

¹ For example, the Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard applicable to organizations that process major credit cards, requires subject organizations to conduct periodic penetration tests. In addition, the National Institute of Standards and Technology resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) provides that penetration testing should be done if reasonable and appropriate.



competitive internationally and less affordable and accessible to U.S. companies and agencies seeking to protect their networks, along with the information about their employees and customers. Furthermore, the Proposed Rule would put US-based security companies that manufacture penetration testing software at a competitive disadvantage to their foreign counterparts, who would not have any of the additional administrative costs associated with managing the sale of these solutions, but could easily incorporate the same exploits into their offering.

The Proposed Rule fails to distinguish between bona fide security products that are designed to prevent misuse and other tools that are prone to misuse

The Proposed Rule would place significant restrictions on exports, reexports, and transfers of penetration test platforms, and would not distinguish between products that possess characteristics and features that deter misuse, and those that do not. For example, as noted above, Metasploit products only incorporate attack methods that are publicly available. In addition, the proprietary editions of Metasploit have a number of built-in safety features intended to ensure that the product is used only for security enhancement purposes. These features include:

- a call-in function that permits Rapid7 to identify where its product is used and to ensure that it is not transferred to embargoed destinations;
- a disabling mechanism that permits Rapid7 to disable an account from receiving exploit updates if the Company determines that the product is being misused;
- the use of extensive logging within the product to ensure that all actions taken by the user can be audited and verified at a later date; and
- the use of encryption to protect the integrity of the logs.

The incorporation of the above safeguards does not interfere with the commercial editions of Metasploit's effectiveness as a security tool, but does make them less attractive to those who would use the product for malicious purposes.

By not distinguishing between products that deter misuse and those that do not, BIS is missing an opportunity to encourage developers of controlled products to incorporate features to maximize accountability and to ensure that their products are used only in legitimate security contexts. We believe that BIS should create a list of features (like those in Metasploit and other products) that, if present, would exempt a product from the proposed controls on intrusion platforms altogether, render the product eligible for favorable license exceptions, or subject the product to less stringent export licensing requirements.

Products that test for zero-day exploits and rootkits are not inherently malicious and should not be subject to a policy of denial

Rapid7 is opposed to BIS's proposed policy of denial for license applications relating to products containing "zero-day exploit" and "rootkit" capabilities. The presence of these capabilities in commercially available penetration testing products does not render such products inherently more prone to misuse. Nor do they determine the defensive or offensive nature of a product. In reality, by their very nature, these kinds of defensive security testing products must simulate offensive tools and tactics. As noted above, we believe that BIS should adopt rules that specify product characteristics that, if present, may exempt an item from the scope of the controls, or render the item eligible for license exceptions or other favorable treatment.

Organizations routinely test their networks to identify potential entry points for attackers, and understand the



impact of an attack. Both zero-day exploits and rootkits play a vital role in this investigation, and so both are frequently found in defenders' toolkits – not just in use by bad actors.

Should BIS disagree and decide to consider the presence of “zero-day exploit” and “rootkit” capabilities when making licensing decisions, we believe that those terms must be explicitly defined. In our view, the terms “zero-day exploit” and “rootkit” should be defined to mean only those exploits and rootkits that are not publicly known or available.

The definitions of “zero-day exploit” and “rootkit” should not be dependent on whether or not a patch for the vulnerability is publicly available, or whether a software developer has taken steps to fix a known vulnerability. Many developers are reluctant to fix vulnerabilities even when they are known, and in other cases there may not be a patch available because the software developer is no longer in business or no longer supports the product. For these reasons, it is the public nature of the vulnerability and the exploit that should be determinative. Once the presence of a vulnerability can be tested for and identified, positive pressure can be placed on the responsible software developer to address the vulnerability and thereby enhance security. Moreover, even if there is no patch, identification of vulnerabilities allows security administrators to make choices about what products they use, how they structure their networks, and what information they put at risk.

Rapid7 submits that the following proposed definitions of “zero-day exploit” and “rootkit” provide the appropriate degree of clarity, while also distinguishing between public and non-public exploit capabilities:

- **Zero-Day Exploit:** A software tool that takes advantage of a security vulnerability that is not publicly known. Security vulnerabilities will be deemed publicly known if: (1) they are the subject of a notice that was made generally available to the public; or (2) they are being actively exploited by criminals.
- **Rootkit:** A non-public, post-exploit software tool that is primarily useful for maintaining control of a computer system without being detected, in a manner that is not authorized by the owner or system administrator of the computer system, after the computer system has been compromised.

The Proposed Rule will have a chilling effect on security research and development efforts

The Proposed Rule does not specifically address security research and vulnerability reporting activities. BIS has stated that its intent is not to interfere with “non-proprietary” research activities (i.e., research activities that are intended to lead to the public identification and reporting of vulnerabilities and exploits). Information and software that is publicly available is not subject to the EAR.

The Proposed Rule, however, would establish controls on “technology required for the development of ‘intrusion software,’” which would regulate exports, reexports and transfers of technical information required for developing, testing, refining, and evaluating exploits and other forms of software meeting the proposed definition of “intrusion software.” This is the type of information and technology that would be exchanged by security researchers, or conveyed to a software developer or public reporting organization when reporting an exploit.

We are concerned that ambiguities regarding the application of the proposed export licensing requirements will have a chilling effect on security research and reporting activities. Accordingly, Rapid7 respectfully submits that BIS should implement explicit and clear protections for activities relating to security research and the public reporting of exploits. Research and reporting activities are vitally important to the development of new and effective security tools.



The absence of license exceptions will make it harder for companies to deploy Metasploit and other controlled products for their own internal use

Currently, security testing products and other items that fall within the definition of controlled items are subject to encryption controls under the EAR. As such, they benefit from license exceptions that permit the distribution of products to and among foreign subsidiaries of U.S. companies for internal use, the hand carriage or temporary export of these tools outside the United States, and the release of certain software products and associated technology to foreign employees of the U.S. company and its foreign subsidiaries.² Under the Proposed Rule, however, exports of controlled items generally would not be eligible for license exceptions under the EAR. As a result, exports that facilitate the widespread deployment and use of security tools within an organization would be barred in the absence of an export authorization issued by BIS. This could lead to delays in the deployment of products, as well as delays responding to attacks. It could also lead to the submission of more voluntary self-disclosures to BIS as security professionals facing attacks are forced to choose between deploying a controlled product internally and waiting for the issuance of a license. Rapid7 strongly opposes any regulatory measures that would make it harder for security professionals to protect their networks.

Real-world scenarios where the rapid deployment of security tools is imperative include:

- Organizations that are high value targets are under constant attack due to the sensitive information they possess (e.g., military technology, personally identifiable information, financial data, trade secrets, etc.). Should use of a new or innovative security tool allow them to better withstand or recover from these attacks, they may not be able to wait for an export license authorizing them to deploy the software to their overseas facilities for their own use and security.
- In the merger and acquisition context, it is customary for acquirers to conduct extensive penetration testing of companies that they plan to purchase as part of the due diligence process. This is done to ensure that threats on the target's network are identified and mitigated prior to integration. In this context, there may not be a sufficient window of time to wait for an export license to test overseas facilities. Once a transaction is announced, attackers will potentially target the acquired company's network as a way into the acquirer.
- An organization on a receiving end of an extortionate threat would need to quickly ascertain the likely impact of an attack, and isolate or protect high value information.

Rapid7 respectfully submits that BIS should authorize the use of Metasploit and similarly controlled security testing platforms by U.S. companies and their foreign subsidiaries in a manner coextensive with Paragraph (a)(2) of License Exception ENC (15 C.F.R. 740.17(a)(2)). Further, we believe that security professionals should be authorized to travel outside the United States with controlled penetration test platforms as tools of trade under License Exception TMP (15 C.F.R. 740.9) or License Exception BAG (15 C.F.R. 740.14).

² For example, penetration testing and other cybersecurity products that utilize encryption are currently subject to export restrictions under the EAR. Paragraph (a)(2) of License Exception ENC authorizes U.S. companies to export specified encryption commodities (including associated software and technology) to any "U.S. Subsidiary." In addition, paragraph (a)(2) of License Exception ENC also authorizes the export or reexport of such items by a U.S. company and its subsidiaries to foreign nationals who are employees, contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use, including the "development" or "production" of new products.



Due to the importance of U.S. Companies to global cybersecurity, it is crucial that BIS get the implementation of these controls correct

BIS's implementation of the Wassenaar Arrangement's agreements on intrusion and surveillance items will have far reaching consequences. Because of the leadership of U.S. companies in the cybersecurity industry, the sheer number of U.S. multinational companies, and the fact that U.S. companies are often the target of cyber-attacks, the impact of BIS's implementation is likely to far outweigh that of other Wassenaar members. For this reason, BIS should not simply follow other Wassenaar members, many of which oversee export control systems that differ markedly from the U.S. in terms of scope (such as the absence of deemed export controls in many European states), resources, and enforcement.

We urge BIS to make every effort to avoid impairing the ability of U.S. companies to develop and market innovative and effective security tools. Further, BIS should seek to affirmatively facilitate (rather than regulate) the ability of U.S. multinational companies to deploy security products for their internal use. This means breaking down barriers to intra-company releases of controlled intrusion products and associated technology.

* * *

We appreciate the opportunity to share our views, and would be pleased to further discuss our concerns with BIS staff.

Once again, given the significant potential impact of the Proposed Rule on a vital part of the cybersecurity industry, we respectfully request that BIS publish another round of proposed controls for review and comment before implementing a final rule.

Sincerely,

Rapid7

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k39-bbak
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0152

Comment on FR Doc # 2015-11642

Submitter Information

Name: Allen Householder

Address:

4500 5th Ave

Pittsburgh, PA, 15213

Email: adh@cert.org

Phone: 412-268-5651

Organization: CERT/CC

General Comment

See attached file(s) for detailed comments.

In summary, we recommend the following:

1. Were experienced in the security research field, but not in the export control field. We reviewed the proposed rules carefully, but we dont understand some important aspects of them. We recommend creating a second draft and establishing a corresponding comment period.

2. We are concerned about chilling effects on vulnerability discovery and disclosure. Such chilling effects could impair vulnerability remediation and management.

3. Difficulty and ambiguity in defining what software (technology) is meant to be covered is likely to have the unintended consequence of chilling beneficial public security research. To ease this risk, we recommend the following:

a. Avoid the use of the terms zero-day exploit capability and rootkit capability entirely as (1)

they are not well defined and (2) they do not sufficiently define a certain class of intrusion software.

b. Define carrier class IP network clearly using well-defined technical metrics.

c. Clarify what is meant by externally provided instructions.

4. We offer our assistance to further refine the proposed rules.

Attachments

CERT_BIS-2015-0011



Software Engineering Institute
Carnegie Mellon University

COMMENTS ON BUREAU OF INDUSTRY AND SECURITY PROPOSED RULE

WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS IMPLEMENTATION: INTRUSION AND SURVEILLANCE ITEMS

Allen Householder <adh@cert.org>

Art Manion <amanion@cert.org>

2015-07-20

About CERT

The CERT Coordination Center¹ (CERT/CC) is part of the Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC) based at Carnegie Mellon University. The CERT/CC was established in 1988 and has decades of experience in software and network security. We engage regularly with the software development (“vendor”) and security research communities in two primary areas of focus:

- Developing tools and techniques for finding vulnerabilities, generally intended for use by software development organizations to improve their security testing
- Coordinating the public disclosure of vulnerabilities among the security research and vendor communities, with the goals of improving processes and developing longer term mitigation strategies

We offer the following comments in response to the proposed rule with request for comments, on the *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, published in 80 FR 28853 [Docket No. 150304218–5218–01] RIN 0694–AG49 BIS-2015-0011.

¹ <http://www.cert.org/>

Summary of Recommendations

In summary, we recommend the following:

1. We're experienced in the security research field, but not in the export control field. We reviewed the proposed rules carefully, but we don't understand some important aspects of them. We recommend creating a second draft and establishing a corresponding comment period.
2. We are concerned about chilling effects on vulnerability discovery and disclosure. Such chilling effects could impair vulnerability remediation and management.
3. Difficulty and ambiguity in defining what software (technology) is meant to be covered is likely to have the unintended consequence of chilling beneficial public security research. To ease this risk, we recommend the following:
 - a. Avoid the use of the terms "zero-day exploit capability" and "rootkit capability" entirely as (1) they are not well defined and (2) they do not sufficiently define a certain class of intrusion software.
 - b. Define "carrier class IP network" clearly using well-defined technical metrics.
 - c. Clarify what is meant by "externally provided instructions."
4. We offer our assistance to further refine the proposed rules.

General Comments

Fundamentally, the Wassenaar Arrangement (WA) definition of “intrusion software” is overly broad. We generally agree with the argument and proposed alternative (“exfiltration software”) described by Bratus et al.²

Our comments align most closely with question #3:

Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company’s ability to protect your own or your client’s networks? If so, explain how.

Our government sponsors have tasked us with coordinating the public disclosure of vulnerabilities among the security research and vendor communities, with the goals of improving processes and developing longer-term mitigation strategies. We are concerned that overly general and imprecise language in the proposed rules could have unintended chilling effects on beneficial security research, thereby inhibiting our ability to perform this important task.

The Intrusion and Surveillance Items FAQ³ provided by the Bureau of Industry and Security (BIS) after the initial FR posting helped to clarify a number of our concerns, for example, by listing exemptions for published research and the exchange of proof-of-concept exploits, malware, and some non-public vulnerability information.

Unfortunately, even with the FAQ and considerable effort, we do not understand some important aspects of the proposed rules. We are also aware of confusion and concern within the security research community, and suggest an additional draft of the proposed rules and a corresponding public comment period.

² <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>

³ <https://www.bis.doc.gov/index.php/policy-guidance/faqs?view=category&id=114#subcat200>

Chilling Effects on Beneficial Security Research

Open, public research in software security benefits the United States and society in general, including the software industry, the defense industrial base, and many elements of the nation's critical, financial, and social infrastructure. Greater use of commodity and commercial off-the shelf (COTS) components in emerging, non-traditional computing markets (e.g., Internet of Things, industrial control systems, medical devices, transportation) increases system-wide susceptibility to vulnerabilities.

Public security research leads to improved software through the resolution, mitigation, and notification of vulnerabilities. Vulnerabilities cannot be resolved or mitigated unless they are discovered and disclosed. In federal government vulnerability management terms, the following steps are involved:

1. Security research is performed.
2. Researchers privately share information about vulnerabilities, exploits, and associated technology with vendors.
3. The results of security research are published, often in the form of public vulnerability disclosures.
4. Common Vulnerability and Enumeration (CVE)⁴ assigns identifiers (CVE-IDs) to publicly disclosed vulnerabilities, and entries are made in the National Vulnerability Database (NVD)⁵.
5. Federal civilian vulnerability management programs such as Continuous Diagnostics and Mitigation (CDM)⁶ and military programs like Information Assurance Vulnerability Management (IAVM)⁷ track vulnerabilities using CVE-IDs.
6. Vulnerabilities are identified, detected, and resolved in deployed systems.

This process is common practice (with different programs for step 5) and is not limited to the U.S. government. Decreasing public research output (steps 1-3) would almost certainly lead to decreased vulnerability resolution (step 6).

Vulnerability research is performed by a wide range of participants from students, hobbyists, and amateurs through professionals with or without advanced degrees, and by both individuals and organiza-

⁴ <http://cve.mitre.org/>

⁵ <https://nvd.nist.gov/>

⁶ <http://www.dhs.gov/cdm>

⁷ IAVM overview: http://www.prim.osd.mil/cap/iavm_req.html

IAVM to CVE mapping: <http://iase.disa.mil/stigs/Pages/iavm-cve.aspx>

tions. Vulnerability research is often performed outside the context of any contractual obligations. Serious vulnerabilities have been found because someone noticed something interesting, pursued it, and took action, not because they were hired to do so. Publication venues range from simple email to a public list, tweets, and blog posts up to rigorous peer-reviewed academic conferences or journals.

Some security research is reimbursed after the fact by bug bounty programs that pay out once a vulnerability has been reported and fixed. Bug bounty programs show promise in helping to identify and remove vulnerabilities. The global nature of the Internet coupled with geographical arbitrage results in many vendors receiving a significant number of vulnerability reports from researchers in other countries.

Legal, regulatory, and policy-making efforts face challenges in keeping up with rapidly evolving technical developments, including security research. Imprecise or outdated legal and regulatory language can lead to chilling effects, as those who would otherwise conduct research may choose not to engage in, share, or publish research due to concerns about legal repercussions.

Concerns Regarding Vulnerability Disclosure for Platform Security

Some vendors offer higher bug bounty payments for reports of vulnerabilities in their platform-wide security features (e.g., exploit mitigation⁸ or sandbox bypasses⁹). To demonstrate the existence of such vulnerabilities, it is often necessary for the researcher to create a proof-of-concept exploit that is indistinguishable from the WA definition of intrusion software, specifically, “Software specially designed or modified ... to defeat ‘protective countermeasures’ ... of a computer or network-capable device, and performing ... the modification of system or user data.” Thus, by providing the vendor with detailed information about the platform security vulnerability the researcher would be transferring “technology required for the development of intrusion software.”

We believe this interpretation to be consistent with the answer to FAQs #19 and #24. We quote the latter for discussion purposes:

The exploit code itself may be considered “intrusion software.” Neither the disclosure of the vulnerability nor the disclosure of the exploit code would be controlled under the proposed rule. However, information for the development of “intrusion software” that may accompany the disclosure of the exploit may be described in proposed new ECCN 4E001.c.

⁸ Microsoft Mitigation Bypass Bounty and BlueHat Bonus for Defense Program
<https://technet.microsoft.com/en-us/Library/dn425049.aspx>

⁹ Chrome Reward Program Rules (Sandbox Escape)
<https://www.google.com/about/appsecurity/chrome-rewards/>

We are concerned that tools used for research and development of proof-of-concept exploits against platform security (e.g., exploit mitigation or sandbox bypass) might qualify as “technology required for the development or production of intrusion software.”

The proposed rules appear to make it illegal, absent the possession of a license, for

1. a U.S. researcher to provide such vulnerability information to a foreign vendor
2. a U.S. researcher to provide such vulnerability information to a foreign citizen employed by a U.S. vendor
3. a U.S. employee of a U.S. vendor to provide such vulnerability information to a non-U.S. employee at that the vendor’s international division
4. a U.S. employee of a U.S. vendor to provide such vulnerability information to a foreign citizen employed in the same U.S. location
5. a U.S. researcher traveling to another country (for example to attend a conference), while in possession of vulnerability research prototypes, meeting the definition of “technology required for the development of intrusion software”

In particular, the second scenario describes the situation in which a researcher discovers an exploit mitigation bypass technique and reports all the details they have (including code) to Microsoft’s Mitigation Bypass Bounty. Would sharing the details with the product security incident response team (PSIRT), which may include non-U.S. citizens, qualify as a deemed export? Is it incumbent on the researcher to first ascertain the citizenship of the PSIRT members who will receive those details? Is it Microsoft’s responsibility to acquire a license for each of their foreign citizens working in their PSIRT prior to receiving the details? Should vendors instead only employ U.S. citizens in their PSIRTs?

It is not clear that the proposed rules are intended to require licensing for the cases described above. We are concerned about the potential for the misinterpretation of the BIS’ intent given the wording of the proposed rules. Such misinterpretation will likely lead many small organizations and individual security researchers to avoid an ambiguous legal context and simply cease performing or privately sharing the results of their research.

We recommend BIS provides further clarification.

Questionable Applicability of Publication Exception

We understand that intrusion software itself is not covered by the proposed rules. Furthermore, we understand that technology required for the development of intrusion software is covered, unless that technology is published. There are common security research scenarios in which both intrusion software and technology required for the development of intrusion software are exported without publication or intent to publish in the future. For example, vendors often release fixed software and publish summary information about vulnerabilities, but they do not publish the proof-of-concept exploits or detailed vulnerability information.

Several FAQ entries (i.e., #4, #10, #19, #24, #25) discuss these scenarios. In particular, FAQ #25 states:

...if technology "required for the development of intrusion software" (as described in the proposed control list entry ECCN 4E001.c.) exported with the functional proof of concept/"intrusion software" would be described in new control list entry ECCN 4E001.c and would, under the proposed rule, require a license...

Consider the following additional scenario: A U.S. researcher reports a technique for exploit mitigation bypass to a non-U.S. vendor with the intent that the vendor will improve the exploit mitigation techniques in their products. From the example in the previous section, we understand that this would constitute “technology required for the development of intrusion software.” However, in such cases often neither the researcher nor the vendor has any intention to publish the technical details or proof-of-concept code the researcher provided. The vendor improves their exploit mitigation technology in a future version. Did the U.S. researcher need to acquire a license prior to reporting to the vendor?

As the above scenario illustrates, vulnerability reports are often accompanied with more information than is actually published upon their resolution. This fact, coupled with the ambiguity of what specifically is and is not covered is concerning. From FAQ #19:

...it is possible that certain technology associated with the exploit would be "technology required for the development or production of intrusion software" under proposed ECCN 4E001.c. As stated in the answer to FAQ #10, any technical data that is transferred with the intent that it be published would not be controlled. However, as the question recognizes, not all technical data is intended to be made public, and some of it may be controlled.

The distinction between proof-of-concept exploit code that qualifies as intrusion software, and associated “technology required for the development or production of intrusion software” is unclear.

We recommend BIS provide further clarification.

Imprecise Language

Our remaining concerns chiefly involve imprecise terminology and language that, left open for interpretation, is likely to cause chilling effects on legitimate, beneficial security research.

The following terms, as they appear in the proposed rules, the WA text itself, or the BIS FAQ, are offered without definitions:

- “Items that have or support rootkit or zero-day exploit capabilities”
- “Describe how rootkit or zero-day exploit functionality is precluded from the item”
- “Support rootkit or zero-day exploit functionality”
- “Carrier class IP network (e.g., national grade IP backbone)”
- “Externally provided instructions”

The absence of definitions as part of the proposed rules significantly inhibits our ability to reason about the rules themselves. Because of this confusion, we request that the BIS revise the proposed rules and corresponding guidance based on the feedback received in this comment period and offer the public a second comment period on the revisions.

Ambiguous: “Rootkit and Zero-Day Exploit Capabilities”

Section 742.6(b)(5) [excerpted for clarity] states

Applications for exports, reexports and transfers of cybersecurity items [list of specifics removed] will be reviewed favorably if [a number of caveats for regional stability], except that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.

Also, in Supplement No. 2 to Part 748, paragraph (z), question (1)(iii)(C)

(C) For items related to “intrusion software,” describe how rootkit or zero-day exploit functionality is precluded from the item. Otherwise, for items that incorporate or otherwise support rootkit or zero-day exploit functionality, this must be explicitly stated in the application.

The adjective “zero-day,” used to modify “exploit,” is generally, loosely understood by security professionals to indicate a sense of surprise by stakeholders (typically vendors), the general security community, or the public. “Zero-day” is not, however, sufficiently precise for use in standards, law, or regulation, including the BIS proposed rules. Security experts do not precisely agree on what “zero-day” means. Appendix A lists ten definitions for “zero-day” from ten different expert sources.

We interpret that the BIS may use “zero-day” to mean exploitation of a vulnerability that is not known to some combination of the victim, the vendor, or the general public, and for which a patch or update does not exist (i.e., the victim would be very unlikely to be able to defend against the exploit, and the exploit would be very likely to succeed).

However, we observe that from the perspective of someone creating a tool to perform penetration testing, vulnerability scanning, vulnerability discovery, or even intrusion software (as defined), there is nothing intrinsic to what the tool does or the knowledge that it embodies that lets its author distinguish between its *zero-day exploit capability* and its *exploit capability*. This ambiguity is entirely because any definition of “zero-day” is an assertion about specific humans’ (vendors, the security community, or the public, depending on the specific usage) ignorance at a particular point in time, and not an assertion about software, its vulnerabilities, their exploits, or any other intrinsic property of the code.

In other words, it is not possible to meaningfully differentiate software that exploits *known* vulnerabilities from software that exploits *unknown* ones. If the intrusion software uses exploits, those exploits may or may not be known to a given party or the general public. Nothing about the intrusion software changes based on others’ state of knowledge.

Contrary to the BIS assertion in FAQ #15, “BIS does not anticipate receiving many, or any, export license applications for products having or supporting zero-day capabilities,” it is our opinion that any technology that supports or provides *exploit capability* must also be presumed to include *zero-day exploit capability* since the differentiating factors occur in the world, not in the technology.

As a result, we strongly recommend that the BIS avoid the term “zero-day exploit” in both the final rules and the supplementary information that accompanies them.

Likewise the term “rootkit” is similarly imprecise and subject to widely variable interpretation. We interpret that the BIS may use “rootkit” to mean a specific kind of intrusion software (as defined) with the features of persistence and stealth. We note that stealth (in the form of avoiding detection) is already part of the definition of “intrusion software.”

We recommend that the BIS avoid the term “rootkit” in both the final rules and the supplementary information that accompanies them.

We further suggest that the rules and supplementary information could be improved by expressing the distinguishing features in terms of some combination of persistence, stealth, exfiltration, remote control, robustness of the exploitation techniques, and reliability of the of the intrusion software. We offer the following definitional sketches that may be useful:

- *Persistence* - designed to persist on an affected system or in an affected network beyond the termination of its delivery mechanism (This could include mechanisms for recovering after a machine reboots, or for reinfection of systems across a network.)
- *Stealth* - designed to evade detection, whether in transit, during execution, or at rest
- *Exfiltration* - designed to surreptitiously send data from the affected system, software, or device without the knowledge of its owner or operator

- *Remote control* - accepts commands from a remote operator
- *Robustness of exploitation techniques* - the ability of an exploit to consistently function and succeed in the presence of platform exploit mitigation technology (ASLR¹⁰, DEP¹¹, etc.)
- *Reliability of intrusion software* - the ability to ensure predictable behavior and performance of the intrusion software

We do not claim that these definitions are sufficiently precise as written. Nor do we offer any specific suggestion for how these terms might be combined into guidance to differentiate export-controlled technologies from non-controlled ones. Our reticence to make more detailed recommendations stems from our lack of understanding of which distinguishing features BIS had in mind. The next section discusses this in more detail.

Did BIS Intend to Discriminate Between Offensive and Defensive Technologies?

We interpret that the BIS intended to define a particular class of technology that is not only controlled but for which no license would be granted (“presumptive denial”). FAQ #22 sheds some light on this intention:

Rootkit and zero-day exploit functionality are features more likely to be found in offensive systems or products. A zero-day exploit is not itself controlled. However, when a rootkit or a zero-day exploit is incorporated into a product or system that is described in the new Category 4 control list entries, or if an exploit delivery tool is specially programmed to deliver or command this specialized malware, that product or system is presumed to be offensive by design.

If BIS’ concern is to distinguish between offensive and defensive security products, with the intent to catch the former while releasing the latter, we believe there is significant work to be done in clarifying the difference and defining the distinguishing characteristics. As it stands the rules, supplementary information, and FAQ left us unable to discern what the discriminating characteristics might be for this class of technology.

To that point, FAQ #13 states, “It is BIS’s understanding that there is no technical basis to distinguish defensive products from offensive products (i.e., a defensive product may be used offensively).” We agree. We are unaware of material technical differences between legitimate penetration testing tools, which incorporate the above features and the class of attack tools that we believe the BIS is trying to define.

For this reason we posit that the “policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities” is untenable in its present state. Given the significant number and depth

¹⁰ Address Space Layout Randomization

¹¹ Data Execution Prevention

of concerns described here, we request that the BIS revise the proposed rules and offer the public a second comment period on the revisions.

Undefined: “Carrier Class IP Network”

From 5A001

j. IP network communications surveillance “systems” or “equipment”, and “specially designed” components therefore, having all of the following:

j.1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):

j.1.a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498–1));

j.1.b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and

j.1.c. Indexing of extracted data; and

j.2. Being “specially designed” to carry out all of the following:

j.2.a. Execution of searches on the basis of ‘hard selectors’; and

j.2.b. Mapping of the relational network of an individual or of a group of people.

Note: 5A001.j does not apply to “systems” or “equipment”, “specially designed” for any of the following:

a. Marketing purpose;

b. Network Quality of Service (QoS); or

c. Quality of Experience (QoE).

Technical Note: ‘Hard selectors’: data or set of data, related to an individual (e.g., family name, given name, email or street address, phone number or group affiliations).

The term “carrier class IP network (e.g., national grade IP backbone)” is undefined. The BIS discusses this in FAQ #14:

The term “carrier class IP network” is meant to specify systems that sit at a national level (or large regional) IP backbone and handle data from an entire city or country. In terms of IP network surveillance systems, this is meant to exclude systems that can only handle smaller data streams or networks, such as those for a campus or a neighborhood. This control does not capture systems that can only analyze data from one person or a small group of people at a time. The term “carrier class IP network” was not defined because it was difficult to put precise technical parameters around this concept.

We note “The term ‘carrier class IP network’ was not defined because it was difficult to put precise technical parameters around this concept” as a critical weakness in the proposed rules. We further observe that it is incongruous to use the term “smaller” without some scale or point of comparison to measure against.

It’s likely that some enterprise or provider networks are significantly larger than the “national grade IP backbones” of some nations. Internet service in some nations is provided directly or indirectly by the government, while service in other nations is provided by private industry, all with varying degrees of regulation, including provisions for legal surveillance.

We suggest that the BIS rules include modifications or notes to more narrowly define “carrier class IP network,” either based on providing service to the general public or having common carrier status. These changes, however, do not consider the size or throughput of the network, which seems to be the intent of *j.1*. If size or throughput are significant defining characteristics, we suggest that the BIS define some scale in terms of data throughput, whether at a network interconnect or equipment interface level, or the potential available processing power or constructed graph analysis capacity (in terms of number of nodes or links it can reason over)¹².

Additional Exceptions to IP Network Surveillance Software

We note the exceptions for “systems” or “equipment”, “specially designed” for any of the following:

- a. Marketing purpose;*
- b. Network Quality of Service (QoS); or*
- c. Quality of Experience (QoE).*

We also suggest that similar consideration be made explicit for

- d) Network availability monitoring
- e) Network performance monitoring

¹² We note that any such definition will necessarily have a limited time horizon in which it remains useful before available technology overtakes it. Thus, continued vigilance on the part of the BIS would be required to maintain the proper differentiating parameters given advances in available technology. We also speculate that horizontal scaling techniques may make any such definition dependent on choices made at the time of such a system's deployment (e.g., how many machines to deploy) rather than being an intrinsic property of the technology (i.e., the same technology deployed as a 100-node instance may be permissible but not as a 1000-node installation). All this is obviously suboptimal to some other decision criteria based on explicitly defined features that such a system offers; however, it seems unlikely that such a definition is possible without reference to system capacity and scaling. We hope to be proven incorrect on this last point.

- f) Network Intrusion Detection¹³ (IDS)
- g) Network Intrusion Prevention (IPS)
- h) Data Loss Prevention (DLP)
- i) Cross-Domain Solutions (CDS)
- j) Network troubleshooting

Ambiguous: “Externally Provided Instructions”

§772.1 defines “intrusion software” using language from the WA with additional notes from the BIS.

(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Our concern with this clause is that the terms “externally provided” and “instructions” may be misleading.

“Instructions” may refer to either (1) machine instructions such as the Intel 64 and IA-32 instruction sets or (2) arbitrary code or commands issued by a remote operator. In the context of the execution of a control-flow exploit such as a buffer overflow leading to provision of a shell, an attacker may use the former to enable the latter.

We interpret that the BIS meant to use the second definition above, and therefore suggest adding an explanatory note.

Furthermore, “externally provided” could refer to either (1) external to the running program or process being exploited, yet still within the same machine, device, or system or (2) external to the machine, device, system, network, or other infrastructure in which the exploited program or process is running.

Again, we interpret that the BIS meant to use the second definition, and therefore suggest adding an explanatory note. If or when there is an opportunity to modify the WA language, we might suggest “...execution of instructions provided by a remote operator,” assuming that is the correct intent.

¹³ Also see Dr. Nicholas Weaver’s comment <http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0089>

Security Assurance for the Licensing Process Itself

Paragraph (z) Part 748, question (2) states:

(2) Upon request, include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.

Software development organizations may be reluctant to share sensitive intellectual property (IP) without safeguards or recourse in the event that the information is leaked or stolen in the course of meeting the proposed rules.

We note the importance of providing sufficient protection to information submitted and subsequently handled in the licensing process. Such protection is important for data both in transit and at rest, whether on the part of the potential licensee, systems involved in the BIS licensing process, or transfer of information to or from reviewers. Given the highly sensitive nature of such submissions, we expect any centralized repositories used in the licensing process to be high-value targets for adversarial entities both foreign and domestic.

We recognize that safeguarding practices may already be well established in other controlled software items such as cryptography. We emphasize its importance here in light of recent significant security events, where the concentration of high-value data has led to catastrophic breaches resulting in precisely the types of knowledge transfer that such processes are specifically intended to avoid.

Appendix A

The following text is reproduced from <https://www.cert.org/blogs/certcc/post.cfm?EntryID=247>

Like Nailing Jelly to the Wall: Difficulties in Defining "Zero-Day Exploit"

By Allen Householder on 07/07/2015

During the Watergate hearings, Senator Howard Baker asked John Dean a now-famous question: "My primary thesis is still: What did the president know, and when did he know it?" If you understand why that question was important, you have some sense as to why I am very concerned that "*zero-day exploit capability*" appears as an operative phrase in the Department of Commerce Bureau of Industry and Security (BIS) proposed rules to implement the Wassenaar Arrangement 2013 Plenary Agreements regarding Intrusion and Surveillance Items.

Background: BIS, Wassenaar, and "Zero-Day Exploit Capability"

The United States Department of Commerce Bureau of Industry and Security recently proposed a set of rules to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013 regarding tools and technologies surrounding "intrusion software."

One particular comment in that proposal is relevant to this blog post: "*Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.*" This policy is implemented in the following line proposed for inclusion in section 742.6(b)(5) [excerpted for clarity]:

Applications for exports, reexports and transfers of cybersecurity items [list of specifics removed] will be reviewed favorably if [a number of caveats for regional stability], except that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.

Further, Supplement No. 2 to Part 748—Unique Application and Submission Requirements—notes the following:

(iii) If the cybersecurity item has not been previously classified or included in a license application, then:

[Other requirements removed for clarity]

(C) For items related to "intrusion software," describe how rootkit or zero-day exploit functionality is precluded from the item. Otherwise, for items that incorporate or otherwise support rootkit or zero-day exploit functionality, this must be explicitly stated in the application.

The answer to question 1 of the BIS FAQ on Intrusion and Surveillance Items reads in part

Transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware would not be included in the new control list entries and would not require a license under the proposed rule.

Later, the answer to question 15 includes this statement:

The only regulatory distinction involving zero-day exploits in the proposed rule regards the possibility that a delivery tool could either have (e.g., incorporate) or support (e.g., be 'specially designed' or modified to operate, deliver or communicate with) zero-day exploits. If the system, equipment component or software at issue has or supports zero-day or rootkit capabilities, then BIS could request the part of the software or source code that implements that capability. BIS does not anticipate receiving many, or any, export license applications for products having or supporting zero-day capabilities.

In writing this post, I attempted to draw a flowchart to map the decision process to discriminate between tools having *zero-day exploit capabilities* but not *exploit samples*, *exploit proof of concepts*. I also tried to generate the possible combinations of both the existence of and vendor and public awareness of vulnerabilities, exploits, and patches, and map those onto whether or not they qualified as "zero-day exploits" or "zero-day vulnerabilities." I failed in both cases.

The reasons I failed are twofold:

1. There are many definitions of *zero-day exploit* available. These definitions are not merely diverse wordings that map onto the same concepts; they refer to distinct (albeit related) concepts. In other words, given the same state of affairs in the world, they yield different answers as to whether or not that state meets the definition.
2. Common to all the definitions is a sense of history, summarized as "Who knew what, and when did they know it?" Note its resemblance to Senator Baker's query. The problem is that some information relevant to the definition only becomes available after certain decisions have been acted upon, and thus that information can not have a causal relationship to the decision in the first place.

I cover both points in more detail below following a brief introduction to why this topic is so relevant now.

You Keep Using That Word; I Don't Think It Means What You Think It Means

Many discussions that touch on vulnerability disclosure involve phrases like "zero-day vulnerability," "zero-day exploit," or simply "zero day" or "0day." However, I've noticed that there is a good deal of confusion as to the meaning of these terms. Security professionals have used these terms inconsistently, or at least they've done so in ways that make it unclear about which meaning they're using. Furthermore, inconsistent use of terms in media reports exacerbates confusion and concern among individuals, network defenders, and decision and policy makers. Finally, in the context of laws and regulations, inconsistent definitions of terminology can become the distinguishing factor as to whether or not one has committed a crime.

Normally I wouldn't write an entire blog post on the definition of terms since for most conversational purposes, loose definitions will suffice. However, when those loosely defined terms become the basis for decisions, policies, and regulations, it's important to get it right.

Like Nailing Jelly to the Wall

The BIS proposed rules that specifically refer to *zero-day exploit capability*. Setting aside what it means for something to have *X capability*, I'd like to demonstrate the difficulty in defining this particular *X*: What's a *zero-day exploit*? (For if we can't define *X*, then *X capability* must also remain undefined.) I went looking for definitions, and found a few:

1. "A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack." —SearchSecurity

The first definition is fairly specific, even if it doesn't really explain what "generally known" means. (Known to whom? What subset of the population must know about it for it to count as "generally known"?) But the rest of it is pretty clear: if the exploit is used on the same day that the vulnerability became "generally known," then it's a zero-day exploit.

Oh, but wait, does *same day* mean the same calendar day? In what time zone? Like the song says, "It's Five O'Clock Somewhere." So if the vulnerability is reported at 11:59 p.m. in your time zone and an exploit is reported five minutes later, is it still a *zero-day exploit*? Maybe?

What if we replace *same day* with *within 24 hours*. At least then we can say for certain that if the vulnerability is made public at 8:00 a.m. UTC on day 0 and the exploit is reported at 8:01 a.m. UTC on day 1, it's not a *zero-day exploit*. I don't know about you, but that strikes me as arbitrary and unsatisfying.

By the way, nothing in this definition talks about patch availability. We'll come back to that in a moment.

2. "A zero day exploit attack occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator." —Kaspersky

There's that *same day* again. I'll grant that *weakness* here is equivalent to *vulnerability* in definition 1. But this definition goes beyond just talking about a vulnerability and its exploit; it mentions a *fix* that *becomes available*.

Stating it explicitly: if the following events occur (a) a vulnerability is announced by a vendor, (b) a patch is provided along with the announcement, and (c) it is exploited on the *same day* (whatever you decide that means, just be consistent), definition 1 says it's a zero-day exploit while definition 2 says it isn't.

3. "An attack on a software flaw that occurs before the software's developers have had time to develop a patch for the flaw is often known as a zero-day exploit. The term "zero-day" denotes that developers have had zero days to fix the vulnerability. It can also refer to attacks that occur on the same day (day zero) a vulnerability is disclosed. In fact, some zero-day exploits are the first indication that the associated vulnerability exists at all." —Tom's Guide

There are two distinct definitions here: one is in the first sentence, and one is in the third. The third sentence equates to definition 1 above, so let's focus on the one in the first sentence.

Here we find that the definition hinges on the existence of a patch. A strict interpretation of this definition would permit someone to apply the zero-day exploit label even if the vulnerability is known to the vendor and the public long before the first attack. The vulnerability may have been known to the vendor for months, and a patch is in development but does not yet exist. Thus definition 3 directly conflicts with both definitions 1 and 2 above. Definition 1 says nothing of patches. Definition 2 talks about patch availability, not existence.

4. "Zero-day attacks...software or hardware vulnerabilities that have been exploited by an attacker where there is no prior knowledge of the flaw in the general information security community, and, therefore, no vendor fix or software patch available for it." —FireEye

Granted, this definition is for a *zero-day attack*, but since it mentions exploitation, I think we are justified to include it here. FireEye adds hardware to our growing list of definitions. Further, they discriminate based on the state of knowledge of the *general information security community*, with the implication that if that community is unaware of the vulnerability, there must not be a patch available. From context, this *general information security community* appears to be larger than the affected vendor(s) yet smaller than the public. So while it shares some degree of overlap with the other definitions discussed above, it remains distinct in its referents.

"But," you say, "these are informal definitions that aren't meant to be interpreted as strictly as you're doing so here." Criticism acknowledged. Using colloquial definitions in a technically focused context may be inappropriate when there are important yet subtle distinctions at play. So let's review the academic literature.

5. "A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning." —Leyla Bilge and Tudor Dumitras, Before we knew it: an empirical study of zero-day attacks in the real world

Again, we make the bridge from *attack* to *exploit*. Interestingly, this definition equates *disclosed publicly* with *unknown*. Yet we know that vendors are continuously made aware of vulnerabilities in their products that the public does not know about: coordinated disclosures are things that happen (and that we here at CERT/CC are often involved in facilitating them).

In this case, *cannot be patched* is not an assertion about the creation of a patch; rather it refers to the application of that patch to deployed vulnerable systems. Also, that point is presented as an implication of the definition rather than a part of the definition.

Interpreting definition 5 strictly, neither of the scenarios presented under definitions 2 or 3 above would qualify as *zero-day attacks*. Definition 4 differs from definition 5 in that it refers to the *general information security community* while definition 5 refers to public disclosure.

6. "A zero-day exploit is a new attack that an organization is not prepared for and can't stop. But there are conflicting definitions of zero-day, and different understandings regarding dates and times when an exploit becomes and/or ceases to be a zero-day exploit. The most practical definition of a zero-day exploit: An exploit that has no corresponding patch to counteract it. Technically, if the exploit code exists before the vulnerability is made public, it's a zero-day exploit -- regardless of how long the software vendor may have been aware of the vulnerability." —Brian T. Contos, *Enemy at the water cooler: True stories of insider threats and enterprise security management countermeasures*

Here we have a definition that at least acknowledges that other definitions exist, then hews fairly closely to definition 3 above.

7. "Zero-day exploit: An attack that exploits a zero-day vulnerability." —David A. Mundie and David M. McIntire, *The MAL: A Malware Analysis Lexicon*

Hmm. Is this definition talking about different things than those presented in definitions 1-4? I can't tell. I suppose we'll have to define *zero-day vulnerability* to figure that out. Conveniently, the MAL defines it for us:

8. "Zero-day vulnerability: A vulnerability that has not been disclosed to the general public and so can be exploited before patches are available."

Exploited prior to public disclosure. Easy enough. Everybody can agree to that, right? Wrong. Keep reading.

9. "A zero-day vulnerability is one that is unpublished. By definition, all vulnerabilities are zero-day before they are disclosed to the world, but practitioners in the art commonly use the term to refer to unpublished vulnerabilities that are actively exploited in the wild. We further distinguish zero-day vulnerabilities from published vulnerabilities as those for which no patch, upgrade, or solution is yet available from the responsible vendor, although some fail to make this distinction. " —Elias Levy, *Approaching zero*

Three different definitions appear here: (a) unpublished, (b) unpublished and exploited, (c) no patch available (regardless of exploitation status). Ugh. One more try?

10. "For the purposes of this paper, we formally define a 0Day vulnerability as any vulnerability, in deployed software, that has been discovered by at least one person but has not yet been publicly announced or patched." —Miles A. McQueen and colleagues, *Empirical estimates and observations of 0day vulnerabilities*

Given this definition we can describe the number of people who know about the vulnerability as greater than or equal to 1 but (significantly) less than *the public*. Also, patch status matters.

Lucky for us, this paper actually prefixes the above definition with the following caveat:

There is no generally accepted formal definition for "0Day (also known as zero-day) vulnerability." The term has been used to refer to flaws in software that no one knows about except the

attacker. Sometimes the term is used to mean a vulnerability for which no patch is yet available.

I'm going to take the hint here and stop trying to pin this down further. You can probably see why I failed in my attempt to map this out in a concise flowchart.

Who Knew What, When?

The thing that is most clear to me from the above is that all definitions of *zero-day exploit* and *zero-day vulnerability* hinge on the state of knowledge of some subset of humanity at some point in time. Once discovered, there is always at least one person who is aware of the existence of the vulnerability. Beyond that the definitions largely vary based on who knows what, and when. This is the connection to Baker's question.

So far, we've established that all the definitions of zero-day exploit and zero-day vulnerability are time dependent. Moreover, they all incorporate the notion of surprise: in order for a vulnerability or its exploit to meet any of the definitions above, its existence must be surprising to someone. Furthermore, the definitions don't simply state that someone has to be surprised they indicate specific subsets of humans that must experience that surprise: either vendors, the security community, or the public, depending on which definition you prefer.

Now, think about that for a moment: What observable property intrinsic to a vulnerability could you point to that tells you this? Nothing. Why? Because surprise arises inside human skulls, not in the software, nor in the vulnerability report, nor in the exploit code, nor in any of the tools that support the discovery or development of these things. The adjective phrase *zero-day* is an assertion about human ignorance *at a particular moment in time*. It isn't an assertion about an intrinsic attribute of software, a vulnerability in that software, or an exploit for that vulnerability.

Complicating things further, not every vulnerability has exactly one vendor responsible for providing a patch. In the CERT/CC, our vulnerability disclosure coordination efforts often require us to work with multiple vendors as we try to synchronize the publication of vulnerability information with the release of patches. In situations where a vulnerability affects multiple vendors' products, public disclosure of one product's vulnerability can lead directly to the users of other products being put at risk because they are exploitable without recourse until a patch for their software is provided.

Even this scenario is too simple though. Some vulnerabilities affect *multiple products* from multiple vendors. This is a common occurrence for vulnerabilities that arise above the code level (e.g., protocol vulnerabilities) or when code is shared across products (e.g., third party libraries, example code that everybody copied and pasted, even a single developer who recreated the same error in multiple projects). So now we have a number of vendors and potentially distinct user groups that could be surprised by the existence of a vulnerability or its exploit. Should a vulnerability that affects 100 vendors' products be considered a zero-day if 99 vendors announce patches while one doesn't? What if 50 vendors patch and 50 don't? What if one vendor provides patches but 99 don't? What if that one vendor accounts for 90% of the users? 80%? 50%? 20%? 2%?

Most extant definitions of *zero-day exploits* and *zero-day vulnerabilities* completely fail to acknowledge this sort of multiparty process, and assume (naively) that a vulnerability report is between one vendor and one finder.

Conclusion

If you discover a vulnerability in a product and you want that vulnerability to get fixed, there's really no way around telling the vendor about it. At the point you make that decision though, you don't (and can't) actually know whether this particular vulnerability is new to them or not. If you find a vulnerability and for whatever reason you don't want it to get fixed, you still don't (and can't) know whether it is unknown to the vendor. You might have some degree of belief about that proposition, but the available facts are limited.

Likewise, the decisions you make to defend your network may be different given your knowledge (or lack thereof) of vulnerabilities, their exploits, and patches. If you have been exploited, you have work to do regardless of the availability of a patch. Whether the vulnerability or exploit deserved the *zero-day* prefix does nothing to help you clean up (although it might help you save face when you get called onto the carpet to explain the attack). Similarly, the availability of a patch gives you a clear course of action regardless of whether you have been exploited or not.

However, from the perspective of someone creating a tool to perform penetration testing, vulnerability scanning, or vulnerability discovery, there is nothing intrinsic to what the tool does or the knowledge that it embodies that lets you distinguish between its *zero-day exploit capability* and its *exploit capability*. As I've shown, all the relevant definitions that could be brought to bear depend on extrinsic factors involving the state of knowledge of others.

In technical contexts, we eschew the use of *zero-day anything* not because it is colloquial but because it is imprecise. Imprecision leads to confusion in technical discussions, and in the current situation, laws and regulations count as technical discussions. Confusion increases costs by creating a drag on decision making. Confusion also leads to a chilling effect as would-be security researchers will avoid performing research that leads to ambiguous legal outcomes and risk of prosecution.

At best, the phrase *zero-day exploit* serves as an attention grabber since it implies that you should pay attention and take some sort of action in response. Using that phrase as a discriminating term as in "a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities" puts individuals and businesses at risk of noncompliance due not to their malicious intent but rather to the incomprehensible wording of the regulation.

It is my conclusion that no definition of *zero-day exploit* is possible that refers only to concepts intrinsic to vulnerabilities, their exploits, and their patches. Thus any tool that supports or provides *exploit capability* must also be presumed to include *zero-day exploit capability* since the differentiating factors occur in the world, not in the tool.

Contact Us

CERT Coordination Center
Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412-268-7090

Web: www.cert.org

Email: cert@cert.org

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0002612

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3a-9st9
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0153

Comment on FR Doc # 2015-11642

Submitter Information

Name: Christian Troncoso

General Comment

BSA submission attached.

Attachments

BSA -- Intrusion Software Comments to BIS FINAL



July 20, 2015 -

Kevin Wolf
Assistant Secretary of Commerce for Export Administration
U.S. Department of Commerce

Hillary Hess
Director, Regulatory Policy Division
U.S. Department of Commerce

Catherine Wheeler
Director, Information Technology Controls Division
U.S. Department of Commerce

**Re: Comments on Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)**

Dear Assistant Secretary Wolf, Director Hess, and Director Wheeler:

On behalf of BSA | The Software Alliance (“BSA”),¹ we write to express the significant concerns of BSA members regarding the proposed rule, with request for comments, issued by the Commerce Department, Bureau of Industry and Security (“BIS”) in the *Federal Register* on May 20, 2015 (the “Proposed Rule”).

The Proposed Rule implicates complex technical and policy issues. BSA urges BIS to pause its current push to issue a final rule, and instead, take the additional time needed to fundamentally consider the proper scope and approach to these controls. Among other steps, BIS should convene technical workshops for input and insight from industry and the security community. After such fact-gathering, BIS should issue a new proposed rule that focuses on a narrower set of items and activities and avoids imposing undue compliance burdens on legitimate cybersecurity efforts. Once those consultations are completed, BIS should issue a second Notice of Proposed Rulemaking so that the cybersecurity community has the opportunity to review and provide comments on the revised rule.

¹ BSA’s members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Datastax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

If implemented as currently drafted, the Proposed Rule would seriously impair the ability of BSA members to identify and fix security vulnerabilities, while requiring thousands of export licenses. The net effect may well be to diminish security for individuals and enterprises because the sheer volume of activities covered under the Proposed Rule would impose unreasonable burdens on the processing capabilities of BSA member companies as well as BIS. As currently drafted, any intended benefits of the Proposed Rule would be overwhelmed by the untenable burdens that it would place on industry and BIS.

Most importantly, we believe the Proposed Rule would hamper the efforts of cybersecurity professionals to protect our nation's critical networks and infrastructure against malicious intrusion by imposing time delays and restricting the use of the best available tools to maintain security, while doing little to impede malicious hackers from obtaining and using tools for cyber intrusions. The Proposed Rule will likely undermine cybersecurity innovation as security researchers and companies alike will be required to seek approval for a broad range of work in a profession that demands its participants move in "Internet time." The Proposed Rule fails to appreciate the global nature of the security community and the important need for international collaboration, within a company and in the security research community. An inflexible regime that is based on nationality means that systems that need protection in real-time are not afforded the best protection available because of the need for licensing and approval.

I. The Overbroad Scope of the Proposed Rule Would Negatively Affect Cybersecurity

BSA understands that the original intent for these controls, when proposed for the Wassenaar Arrangement, was to restrict the export of sophisticated surveillance systems — such as those developed and sold by FinFisher and Hacking Team — to authoritarian governments, which reportedly have used these systems to spy on or otherwise repress political dissidents and other citizens.² BSA agrees that such systems, which permit the targeting and monitoring of an individual's phone calls, emails, and other communications, are appropriate items for tight export controls, implemented by the United States, the European Union, and other Wassenaar members.

By contrast, the scope of the Wassenaar controls as proposed for implementation in the Export Administration Regulations ("EAR") by BIS, would apply to a far broader range of items and activities. For example:

- *Technology Controls.* Export Control Classification Number ("ECCN") 4E001.c would control "technology" "required" for the "development" of "intrusion software." Because this ECCN entry lacks specific performance levels, much of the technology related to the development of intrusion software likely would qualify as "peculiarly responsible for

² See, e.g., Bill Marczak, Written Evidence to the UK Parliament, *Export of British-Made Spyware Targeting Bahraini Activists* (Nov. 19, 2012), available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmfaaff/88/88vw43.htm>; Response of the UK Secretary of State for Business Innovation and Skills, *Export Controls for Surveillance Equipment - Proposed JR* (Aug. 8, 2012), available at https://web.archive.org/web/20140816043658/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_08_08_response_from_tsol.pdf.

achieving or exceeding the controlled . . . characteristics or functions” of “intrusion software,” and therefore would be considered “required” for its development. As a result this ECCN would describe an exceedingly large range of technologies, with virtually all exports and re-exports of such technology requiring an export license.

- *Software Controls.* Similarly, the proposed software controls in ECCN 4D004 attempt to limit their scope by only applying to software “specially designed” or modified for the generation, operation or delivery of, or communication with intrusion software, rather than intrusion software itself. However, BSA members report that all intrusion software that is developed for defensive/security purposes needs to be generated, delivered, and communicated with in the process of testing (and fixing) network and software security vulnerabilities. As such, BSA members report that they frequently develop and export software that would be controlled under ECCN 4D004 (as well as ECCN 4D001), both manually and through auto-code generation.

BSA appreciates the efforts that BIS has made to clarify the intended scope of the Proposed Rule, including the scope of these ECCNs, in a series of responses to Frequently Asked Questions (“FAQs”) on the BIS website. However, these FAQs are not reflected directly in the language of the Proposed Rule, and do not have the force of law. More importantly, even taking these FAQs into account, BSA members report that technology and software covered by these ECCNs are frequently generated by BSA members in the course of efforts to identify and fix network, software, and other security vulnerabilities, including critical cybersecurity work to protect our nation’s IT infrastructure. Because of the global nature of defensive security activities, and the wide involvement of security professionals of many nationalities, these activities require exports and re-exports to intra-company and third-party security teams in European and other countries, as well as “deemed exports” to non-U.S. nationals (lawfully working in the U.S.) and “deemed re-exports” to dual and third-country nationals lawfully working in non-U.S. countries. Moreover, these deemed exports and re-exports must occur globally and within minutes, given that vulnerabilities or threats may require tooling, software, and expertise to move as quickly as the threat.

II. The Proposed Rule Would Result in Thousands of Export License Applications

The burden of complying with the Proposed Rule would be substantial. As drafted, the rule would require licenses for virtually all exports, re-exports, and deemed exports of an overly-broad set of controlled items. Some BSA members have projected that, if the Proposed Rule is adopted, their individual companies would likely be required to obtain thousands of export and/or deemed export licenses. The number of licenses required across all BSA member companies would be much larger, and the projected number of activities and tools subject to licensing controls in the software and IT industries would be staggering. It would bring development and testing to a standstill, as the backlog of licensing requests would quickly balloon to an unmanageable level. This volume is unmanageable for even the largest companies’ Trade Compliance departments, and even more importantly, BIS does not have nearly enough capacity to process these license applications.

It is also worth noting that many in the security researcher community lack the resources necessary to comply with the Proposed Rule. Much of the cutting edge work in the

cybersecurity field is performed by sole practitioners, small businesses, and academics. These entities are unaccustomed to the complexities of the export licensing process, and the delays and costs of complying with the Proposed Rule will significantly undermine their ability to participate in the cybersecurity ecosystem. Because many enterprises, including BSA members and governments, rely on their contributions, the impact on the security community will be widespread.

The Proposed Rule will make it exceedingly difficult for industry to identify and segregate controlled from non-controlled technology in the context of ongoing cybersecurity efforts; as such, industry will be forced to be over-inclusive when identifying controlled technology. Furthermore, an exporter would only need to anticipate sharing a single piece of controlled technical data with a foreign national for the export or deemed export licensing requirement to apply. The broad scope of the controls, and the ambiguities that remain even after multiple issuances of FAQs and answers, thus contributes to the massive projected licensing volume that would be created by the Proposed Rule.

The licensing burden results not only from the overbroad scope of the Proposed Rule, but also because the Proposed Rule does not offer any eligibility for license exceptions. For example, the Proposed Rule does not authorize mass-market software exports under License Exception TSU. The Proposed Rule likewise would not authorize exports of software or technology with a written assurance and appropriate compliance measures under License Exception TSR. License Exception ENC also would not be available for cybersecurity items that perform encryption.

It is important that BIS create new license exception(s) to enable legitimate and critical cybersecurity activities, such as intra-company transfers or transfers with third-party partners for security research activities. Such license exceptions are entirely consistent with U.S. participation in the Wassenaar Arrangement. The Wassenaar Arrangement is a forum for member states to agree on *what* is controlled. As explicitly stated in the Wassenaar *Initial Elements*, the decision on *how* to control the export of a controlled item is left to “national discretion.”³ Indeed, the European Union has already implemented the Wassenaar controls,⁴ including the availability of general licenses for certain exports (and subject to compliance with certain additional requirements).

BIS should also reconsider the “policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.” Because most, if not all, end point security products contain some degree of rootkit functionality, a presumption of license denial will impede the ability of cybersecurity professionals to use and exchange a broad range of products and tools that are critical to protecting networks from intrusion. Restricting the exchange of items containing zero-day vulnerabilities and associated exploit capabilities will have a similar effect. Cybersecurity professionals engage in penetration testing for purposes of identifying and remediating network vulnerabilities and exploits. The tools used in penetration testing exercises

³ See Wassenaar Arrangement, *Initial Elements*, Section II.3, available at <http://www.wassenaar.org/guidelines/docs/5%20-%20Initial%20Elements.pdf>.

⁴ See Regulation (EU) No 1382/2014 (effective as of Dec. 31, 2014).

make use of zero-day vulnerabilities and then help to develop exploits to assess those vulnerabilities. The research and software engineering necessary to remediate those exploits is conducted in hours and is international in scope. To effectively close those network vulnerabilities, companies must be able to share freely and in real time. The inability to freely share the vulnerabilities and exploits that the penetration testing tools find, due to their zero-day exploit capabilities, will severely impact the ability to create safe products and ensure a secure network and IT environment.

III. BIS Should Fundamentally Rethink the Approach to these Controls and Issue a Second Proposed Rule

BSA recognizes that the goal of the Proposed Rule is to protect human rights by preventing rogue actors from undermining cybersecurity. However, by imposing enormously burdensome requirements on fundamental network security tools and practices, the Proposed Rule is likely to have the opposite effect. Securing systems and individuals against exploits, vulnerabilities, intrusions, and threats requires real-time testing and remediation actions. Such efforts must occur immediately upon the detection of a vulnerability or intrusion. As drafted, the Proposed Rule would impose burdens that will inevitably delay testing and remediation, and thus diminish security in a very real way. Both product development and security response will be stymied, as approval will be needed at each step of the process. Such an outcome would be at odds with the Obama Administration’s broader cybersecurity policy, which recognizes that “private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.”⁵

Given the complexity of the technical and policy issues raised by the Proposed Rule, BSA urges BIS, along with its inter-agency partners, to pause any current rush to issue a final rule. BIS should take the time to fundamentally rethink the approach taken to these controls -- i.e., whether to revisit the scope of the controls at Wassenaar; to issue Technical Notes, definitions, lists of excluded items within ECCN entries; or other options for appropriately drawing the scope of these controls. This also could include BIS hosting technical seminars or workshops with industry and the security community.

In the process of this engagement, BIS may identify novel approaches -- which satisfy the needs of both the U.S. Government, industry, and other organizations -- to regulation in this complex area. For example, as BIS did with encryption exports, and as implemented by the EU, there may be a registration-based approach for cybersecurity items that avoids the need for individual licensing. Alternatively, there may be end-user or end-use-based controls that more effectively control the sensitive activities of interest to the U.S. Government, without over-controlling non-sensitive, security *enhancing* activities. Such an approach could differentiate between “white hat” developers who are seeking to improve security across the ecosystem and “black hat” hackers who are focused on substantially harming an information system or data on

⁵ Executive Order 13691.

an information system. A use-based focus could help to ensure that the export control licensing requirements are not undermining the time sensitive efforts of cybersecurity professionals. However it is constructed, the final rule should be minimally invasive and maximize the ability of the security community to innovate and respond to threats and global challenges.

Once this work is complete, BIS would be in a position to issue a second proposed rule, as has been done with other complex Export Control Reform rulemakings. This second proposed rule should clearly describe the (much narrower) scope of controlled items, without reliance on FAQs on the BIS website (which do not have the force of law) and provide an opportunity for further commentary as needed.

BSA and its members welcome the opportunity to engage further with BIS, and all other interested departments and agencies, on these complex technical and policy issues.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3a-yl30
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0154

Comment on FR Doc # 2015-11642

Submitter Information

Name: Fred Powell

Address:

2038 Greenwich In.

Toledo, 43611

Email: iamfredpowell@gmail.com

Phone: 4195094974

General Comment

I do not understand why you would want to limit progress. What is the upside to this?

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3a-v0uv
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0155

Comment on FR Doc # 2015-11642

Submitter Information

Name: Ryan Corcoran

Address:

14123 76th PL NE

Kirkland, 98034-5069

Email: rcorcoran7+gov@gmail.com

Phone: 4252239475

General Comment

I'm a SOC analyst and I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3b-kyq2
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0156

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

In this era of routine security breaches and cyberattacks, criminalizing the export of code will hamstring the persons available for securing cyberspace - namely, security researchers. We do not currently have the technological means of determining all types of vulnerabilities or mitigation measures. To outlaw mechanisms when cybersecurity is in its infancy would be unwise and potentially disastrous.

I implore you - please do not hamstring security researchers with export controls on code. It will make our future a much less safe one.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3b-n1rh
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0157

Comment on FR Doc # 2015-11642

Submitter Information

Name: Ronnie Tokazowski

General Comment

Hello decision makers,

While it may seem that creating regulations on this may seem to hamper the attacker in the short term, the long term effects of this will be detrimental. Creating "arms" and "export" regulations for software will not stop the problem. The goal should be to make it harder for the attackers to do their work, not make it harder on the folks who are stopping these attacks. Other countries hack away at the economy of the United States left and right, however no actions have been taken against those countries. (See Russia, China, Iran, etc.) Just as we've seen with guns, even with gun regulations, bad guys still have guns. The only difference is that a 12 year old can't create a gun in his basement as easily as they can create a software "weapon".

If this goes through, this is going to create a slippery slope for researchers who are helping stop these attacks on a day to day basis. If company X is hacked and I come across a list of passwords, I can't help them, as I'm now considered a criminal for being in possession of the passwords. If I have a malware sample from an APT group that I'm investigating, I'm considered a criminal, even though that information goes directly to the organizations who can kick the attackers out of their network. Please don't push this through.

Kind regards,

--Ronnie
@iHeartMalware

PUBLIC SUBMISSION

As of: July 27, 2015 Received: July 20, 2015 Status: Posted Posted: July 27, 2015 Tracking No. 1jz-8k3b-1b4c Comments Due: July 20, 2015 Submission Type: API
--

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0158

Comment on FR Doc # 2015-11642

Submitter Information

Name: Timothy Lisko

Address:

1913 Green St

Unit 2

Philadelphia, PA, 19130

Email: timothy.lisko@privacywonk.net

Organization: PrivacyWonk

General Comment

"Having any kind of speed bump to defense actually makes the entire Internet less safe for everyone," ~Katie Moussouris, chief policy officer of HackerOne

Source: <http://www.npr.org/sections/alltechconsidered/2015/07/20/424473107/commerce-department-tighter-controls-needed-for-cyber-weapons>

This regulation will create a giant speedbump for defending our networks if we must seek licensing and approval for export, reexport, and in country transfers of technology. Computer Network Defense (CND) uses the same tools as attackers. CND is already at a significant disadvantage without having to seek a license for a tool, potentially delaying procurement and implementation of said tool. With the Administration's continued focus on security (see NIST Cybersecurity Framework efforts, OMB memorandum, and more) this is a giant step *backward* by regulators who appear out of touch with the technology and their uses. Security professionals must be free to adapt to a constantly changing threat landscape by researching, developing, and deploying new tools and technology without delay to prevent or mitigate an

attack.

"While best practices concerning the need to control the exchange of software were recognized as far back as 2006 there is an inherent difficulty in controlling open-source and free software. As a result, open-source and free software is exempt from control under the Wassenaar Arrangement. As the General Software Note within the Wassenaar Dual Use List makes clear, software generally available to the public or in the public domain is not subject to control (a legacy of the crypto-wars, however, is that this exemption does not apply to cryptographic items)." Source: <https://www.newamerica.org/oti/export-controls-and-open-source-software/>

The proposed rule notes that the incredibly broad list of newly regulated items were not previously designated for export control but some of them may have been because of their crypto operations. This seems like a large jump in the conclusion: "well, because some security items use crypto lets regulate all of them!" Open source tools are absolutely critical to the security community. These tools are often maintained in ad hoc fashion with no principle owner, no one to apply for a license or submit a letter explaining what the software does. As noted above, this would be incredible difficult to control and enforce. I have not become aware of any control / enforcement mechanisms for open source software and items that would have changed in the last nine years.

If the proposed Wassenaar laws pass, the community will adjust over the course of a year or two. If nobody is found to be pursued for Wassenaar violations, then its likely itll be business as usual. If people are pursued, it will likely make it so researchers no longer communicate their findings to vendors and revert the security industry back to 1997 when 0-day exploits were traded in tight knit circles. ~Ryan Smith, Accuvant (security research firm). Source: <http://www.csoonline.com/tag/hackedopinions/>

The attempt to regulate "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices" is a fools errand that will stifle innovation and further weaken our overall security posture. If we cannot share and discuss vulnerabilities freely, we cannot develop the solutions to fix or mitigate them. The Security community relies and lives on this research. We live on information sharing. Without it, we can never know how vulnerable we are. Without penetration testing and curious security researchers we will never know how vulnerable a piece of software or a device is. Ignorance of a vulnerability does not protect, it makes us weaker. It provides an opportunity for a bad actor to know the vulnerability first and to exploit it. Worse, this could give incentive to companies to not invest in security research and lead to less secure products being shipped and delivered. As Ryan mentioned in the quote above, it will stop disclosure and it will kill all progress we have made as a community and industry in the past two decades. I have attached every interview CSO Onlines Steve Ragan conducted with security industry players and their opinions on the topic. The responses do not paint a positive picture for the effects this rule may have.

I strongly state an objection, as a citizen and security professional, to this proposed rule. The impacts are too grave to both public and private CND operations and have not been appropriately considered by regulators.

Attachments

Hacked Opinions_ Vulnerability disclosure – Garve Hays _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Geoff Sanders _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Morey Haber _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Robert Hansen _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Ryan Smith _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Tom Gorup _ CSO Online

Hacked Opinions_ Vulnerability disclosure – Tomer Schwartz _ CSO Online



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Garve Hays

NetIQ's Garve Hays talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 5:00 AM PT
Thinkstock



[NetIQ's Garve Hays talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.](#)

[Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?](#)

[CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.](#)

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Garve Hays (GH), Solution Architect, NetIQ: I stand between full and responsible disclosure. I'm of the opinion that sometimes organizations need a "helping hand" to prioritize security over features.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

GH: With no communication at all or "stone-walling," full disclosure is a proper course of action. As we saw with labor reform following the industrial revolution, we should likewise expect software companies to advance their responsibility in the App Economy.

It is unacceptable to ignore security vulnerabilities, particularly in the face of evidence showing them to be present. The counterpoint is that all parties should reach a consensus that a potential exploit is practical and not merely theoretical. But this will not happen in the absence of discourse.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

GH: Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

I think the expansion of programs like the Linux Foundation's Core Infrastructure Initiative to include bug bounty programs would supplement the ongoing development of open source projects in the critical path of core computing. Regarding companies with limited resources, I am encouraged by "crowd-sourced" initiatives such as Bugcrowd.

[**Note:** Alternatively, organizations and turn to HackerOne for bounty programs as well.]

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

GH: Definitely. Public awareness is a key component in the ongoing effort to protect our data and advance the state-of-the-art. Not everyone follows BugTraq, so the more accessible the information, the better the chance of public scrutiny.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

GH: I'm not sure one can address the Wassenaar Arrangement in isolation without the context of the Computer Fraud and Abuse Act (CFAA), but I'll give it a shot.

So although the Wassenaar Arrangement (WA) applies to the export and sale of "controlled munitions," which in this case now includes so called cyber-weapons, it will impact the disclosure process by adding overhead. Whereas the procedures were formerly mostly cooperative, there is now an imposed layer of bureaucracy.

Regulations are nothing new in the computer security industry, but the cost of an error here may now be applied to individual security researchers as well as a company. A million dollar fine may be tolerable for a large company, but such a fine coupled with a 20-year jail sentence for an individual is sobering.

The community of security researchers is a global one and as such necessitates international transfer of ideas and working code. This can no longer be an informal process. Researchers must plan ahead and release their code prior to traveling to conferences, for example.

I think most participants will adapt and continue to disclose their findings; it just may take longer than before, which is unfortunate due to "Internet" speed. Which is to say that malicious actors and criminals will have no such restraint.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Geoff Sanders

LaunchKey's Geoff Sanders talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 4:00 AM PT

Thinkstock



LaunchKey's Geoff Sanders talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.

Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?

CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Geoff Sanders (GS), Co-Founder and CEO of LaunchKey:

I believe a responsible disclosure policy which allows for full disclosure of a vulnerability, following a brief period to allow patches to be deployed and affected users to be notified, strikes the right balance of the need to fix the problem, inform the public of the risks, and reduce further exploitation, so long as policy owners address disclosures promptly and with urgency.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

GS: Absolutely. The 'responsible' part of responsible disclosure applies as much to the vendor as it does to the researcher. Responsible vendors are prompt and maintain an open dialogue with researchers. If a vendor or CERT goes silent, a researcher has no choice but to assume the vendor isn't addressing the issue at which point it becomes the ethical responsibility of the researcher to fully disclose the vulnerability.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

GS: I think most security researchers simply want a financial bounty that respects the amount of work they've put into finding the bug, and one that's appropriate for the size of the vendor paying the bounty.

Large vendors should offer rewards that at minimum reflect the cost of contracting similar professional services in the market, while researchers should respect that startups and small vendors will have proportionately less capital to reward.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

GS: I don't think every vulnerability needs a cool name and logo, but I think it can definitely help with the more significant vulnerabilities that demand greater attention from the public. Being that the general public isn't a technical audience, it makes sense to market these bugs in friendly and memorable terms for the same reason we refer to Rhinopharyngitis as the common cold.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

GS: Security researchers rely on the ability to recreate vulnerabilities to both discover bugs and build defenses against them.

The proposed changes to the Wassenaar Agreement add vague language which opens up researchers to the potential for prosecution. Such an approach will only serve to dissuade participation from the security research community and limit collaboration between researchers which is paramount to finding and fixing critical vulnerabilities in a timely manner.

At the end of the day, sharing and disseminating vulnerabilities and malware will still be a trivial endeavor, and the bad actors this approach is supposed to impair will merely find vulnerabilities that remain unpatched for longer periods of times that allow greater exploitation.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Morey Haber

BeyondTrust's Morey Haber talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 3:00 AM PT
Thinkstock



[BeyondTrust's Morey Haber talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.](#)

[Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?](#)

[CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.](#)

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Morey Haber (MH), Vice President of Technology, BeyondTrust:

I believe in responsible disclosure. The notification of vulnerabilities to the public should only occur after a mitigation (patch or permanent configuration change) is available from the vendor or open source project. The reason why is simple; to minimize the risk to the end user and business until an acceptable solution is found. The history of full disclosure has shown us that exploits will appear well before anyone can defend themselves and create unnecessary loss financially (time, goods, and outages) when no solution is available. It is kind of like complaining to your boss about a problem but having no solutions to mitigate the issue. Always have a plan to solve a problem when you escalate an issue. Never show up empty handed.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

MH: No. Full disclosure is never an option. As a researcher, persistence and patience is very important. These are traits you must accept as a part of the work you are doing and a risk based on your findings. If no one replies, move on to the next project for all the reasons I listed above. Organizations can go dark for many reasons: the complexity of the issue to resolve, lack of talent and understanding to mitigate the risk, all the way through to pure incompetence.

Full disclosure is not an option for any of them and the work a researcher does is like an artist. Not everyone will appreciate your work, even if it is a masterpiece in vulnerability research or a simple splatter of paint potentially worth millions. A researcher must accept that the work they do may fall on deaf ears or be worth cash.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

MH: Morals. An honest day's work as a researcher in receiving a Bug Bounty is far more ethical than selling the findings of a bug / exploit for misuse. It is the same problem with downloading movies or music. People do it all day but would not walk into a local store and steal a DVD.

The Internet of Things has made cybercrime a much more tolerated crime and selling an exploit much more acceptable. As a society we need to raise the awareness that both are equal crimes even though it does have a physical aspect to it.

To that end, researchers are doing very important work but must be legally ethically responsible with their findings. In order to shortcut this problem, I would encourage vendors and researchers to work together through established companies like Veracode (services) or even Bugcrowd. The later represents a relatively new way to identify these problems and properly handle disclosure and mitigation.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

MH: Yes, but only after Responsible Disclosure. Raising awareness is key at all levels of business / management and society. Only then do we understand the urgency to mitigate the risk and prioritize resources to close the vulnerability from potential exploitation.

If we did not have these media campaigns, potentially only engineers, auditors, and a few other teams would understand the risk and their voices alone may not be loud enough to solve the problem.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

MH: If Wassenaar passes with the current changes, I think you will see a split in research and public disclosure.

I believe the criminal activity for underground exploits will blossom because people that are doing the work secretly can make money from their research and have no real public forum to share their results responsibly. The other half will be employed by companies to conduct the research themselves or via services.

The days of a researcher as a consultant performing full disclosure could be a serious crime as they find other avenues to obtain a capital gain for their work. Basically, any time you make something illegal – the camp splits and you find people on both sides. Think Prohibition.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Robert Hansen

WhiteHat's Robert Hansen talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 3:00 AM PT
Thinkstock



[WhiteHat's Robert Hansen talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.](#)

[Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?](#)

[CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.](#)

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Robert Hansen (RH) Vice President of WhiteHat Labs, WhiteHat Security:

I'm definitely in the middle. There are [types of] vulnerabilities that would cause far more harm than good if they got out. If I know that the vendor in question will act responsibly and close the vulnerability as fast as possible, I'm far more likely to tell them. If I know the vendor in question won't fix the vulnerability quickly, or if I know that the vendor is unethical, I'm more likely to go full disclosure. But for the most part, most companies do their best, and act correctly, so I use responsible disclosure.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

RH: Absolutely. At some point companies have to learn that their customers' security is important and deal with it correctly. And the researcher ultimately will side with the customer because they want the vulnerability closed. If the company refuses to close the vulnerability or respond, what other option do they really have? Let the customers stay vulnerable? That feels ethically questionable.

I've got a long history of going full disclosure against advertising companies as an example. If they're stealing peoples' privacy, I have less interest in protecting them.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

RH: Ultimately this is a supply and demand question - who is going to pay the researcher whatever they want to get paid? Some researchers have ethics that prohibit them from disclosing to anyone other than the company, but if they aren't getting paid enough they'll probably just stop doing the research altogether.

There are many vulnerabilities that are worth a lot to adversaries, and if the company isn't willing to pay fair market value, or even close, it's not a stretch to say that researchers with pure profit motives are going to look to more questionable markets.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

RH: Somewhat. I think for the most part naming vulnerabilities is largely a holdover from virus research, which has a long history of naming viruses. Later it switched to naming vulnerability types and classes as well for convenience. It does make things easier to distinguish and therefore more convenient to talk about. But the hype makes it a bit annoying for researchers who have to deal with the aftermath.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

RH: In most situations it probably won't matter much, but it will impact a handful of companies that do trade in 0days. There is some grey area though, where companies like WhiteHat find 0days in companies' websites on a regular basis. It's unclear how it would affect us and similar companies. Also, there is no accounting for the chilling effect that this type of regulation will have on the industry as a whole.

It won't kill full disclosure. If a researcher wants to go full disclosure, they will certainly find a way. But it may reduce it in cases where individuals don't stand to profit and don't want to risk running into legal issues in the process. The largest effect will be on the end consumer and companies, who will remain vulnerable longer than they need to be, due to the chilling effect.

The question people really need to be asking themselves is, in what way does this regulation actually thwart actual black markets or real adversaries? It's a fairly small subset of people who will care about this regulation that wouldn't also fall under existing regulation. This is more or less a witch-hunt, that provides very little real value to the companies who use vulnerable vendors or the consumers who rely on companies to do the right thing.

It's extremely unlikely that someone who is concerned about the law will do anything other than hoard their knowledge, or go full disclosure over the dark-net. Why risk going public when the legal system appears to want to punish them every chance it gets. This is just another dangerous example of poorly thought out cyber-security legislation that will almost certainly cause more harm than good to an already complex ecosystem. Most well-intentioned cyber-security legislation doesn't stand up against the scrutiny of actual security research needs.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Ryan Smith

Accuvant's Ryan Smith talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 5:00 AM PT
Thinkstock



Accuvant's Ryan Smith talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.

Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?

CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Ryan Smith (RS), Vice President & Chief Architect, Accuvant and FishNet Security:

Full disclosure and responsible disclosure are not mutually exclusive philosophies. Full disclosure is the philosophy that secrecy is bad for security. Responsible disclosure is the philosophy of reducing the potential harm to security. Coordinated disclosure is the practice of coordinating with vendors when publishing vulnerability information.

When discussing the best form of disclosure there are many facets to consider. Vendors differ in their ability to effectively respond to security vulnerabilities. One vendor may have an entire team dedicated to vulnerability disclosure while another may not have anybody tasked to disclosure and has never dealt with disclosure in the past.

The target of the vulnerability research differs tremendously these days as well. Finding a vulnerability in a traditional software product is different than finding a vulnerability in a website, and both differ from finding a vulnerability in an embedded device. Patching is easy and straight-forward in traditional software. With websites like Facebook or Google, it may not benefit anyone to know the details of the vulnerability since only Facebook or Google need to patch. With embedded devices you deal with difficulties addressing the vulnerability.

Sometimes it requires a complete board revision, and sometimes deploying a patch requires boots on the ground to visit millions of locations. To have a rigid, one-size-fits-all policy will unnecessarily cause chaos in some types of systems. It's better to intelligently determine how best to disclose and ensure that your disclosure policy allows enough room to adjust.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

RS: When a researcher is working closely with a vendor to help them fix a vulnerability and the vendor goes silent, it can be frustrating. Did they go silent because they decided not to address the vulnerability? Does the contact have a medical emergency? Or, maybe they disagree with what constitutes a vulnerability?

The point here is that silence is never a good communication option as it usually causes people to synthesize information for themselves. Sometimes, this synthesis causes people to believe that going public with the vulnerability information is the only way to allow people to secure themselves.

In this scenario it's important for the researcher to take a step back and evaluate the situation from an altruistic perspective rather than from the passion created from having spent months discovering the vulnerability. The researcher must really determine how he or she can best help the security of the people who are using the affected system.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

RS: Every researcher has individualized motivations for performing the research and perceives value differently. It's important to consider that performing vulnerability research while not under contract for the vendor is effectively working without getting paid.

My motivation has always been to expand my and the security community's knowledge of how systems work, not to make money. But if I were in it for the money, when you add up all associated costs – devices, hardware software and time, many of the bug bounties appear to woefully undervalue the researcher's time and investment.

Vendors can better engage the knowledge-motivated researchers by creating partnerships and sharing. They could give researchers free access to their hardware, software or service. They could invite researchers into private beta tests.

They could invite researchers to speak with the product development teams. By engaging meaningfully and sharing in-kind the knowledge-motivated researcher could have better access, and be able to serve as a partner, delivering real value.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

RS: When it comes to vulnerability marketing, you have to consider why organizations are undertaking such measures. Vulnerability research is expensive, so companies want to extract the most value from those endeavors. With Heartbleed, I think there was value in giving it a name and promoting awareness of the vulnerability. Some of the marketed vulnerabilities that followed had more questionable value. If you break down the phenomenon of marketed vulnerabilities into elements, there are good qualities and bad qualities.

First, anti-virus companies have been naming malware since their inception. Giving vulnerabilities a memorable, pronounceable name allows better discussion, and allows people to more easily remember the nuances of the vulnerability so the mistake isn't repeated.

If a company were to setup a website, logo and hype the vulnerability to the media more than the vulnerability warranted, that's less productive. It improperly focuses the attention of the security community on things that don't matter, possibly diverting resources from more important vulnerabilities. If the attention isn't unwarranted, and facts aren't skewed, then it doesn't matter if companies throw vulnerability launch parties.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it

see a boom in responsible disclosure out of fear of being on the wrong side of the law?

RS: If the proposed Wassenaar laws pass, the community will adjust over the course of a year or two. If nobody is found to be pursued for Wassenaar violations, then it's likely it'll be business as usual. If people are pursued, it will likely make it so researchers no longer communicate their findings to vendors and revert the security industry back to 1997 when 0-day exploits were traded in tight knit circles.

The proposed Wassenaar laws, as they're written and as I understand them, make it so that disclosure of vulnerabilities to an organization outside of the US would require an export license for each disclosure.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Tom Gorup

Rook Security's Tom Gorup talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 5:00 AM PT
Thinkstock



[Rook Security's Tom Gorup talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.](#)

[Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?](#)

[CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.](#)

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Tom Gorup (TG), Security Operations Manager, Rook Security:

Responsible Disclosure. I believe developers are going to make mistakes and in some cases the functions they have imported are the issue, not necessarily the code itself. Developers/companies need an opportunity to resolve this issue prior to release. However, there should be a deadline applied to this solution.

Just because it hasn't been publicly released does not mean it's not being actively exploited. The general public needs to know in a timely manner in order to apply local mitigations through available tools, or at minimum a way to detect if the activity has occurred within their environment.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

TG: Yes. The general public needs to be aware of these vulnerabilities. As I said above, just because the vulnerability has not been publicly disclosed does not mean it's not being actively exploited. Companies need a chance to defend against these attacks. If they don't know the vulnerability exists, how can they possibly defend against it?

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

TG: This is a tough problem. The underground market for exploits will always outbid the general industry. Companies can't afford to keep up with these cost. However, I don't believe the bounty programs are marketed enough.

Getting the word out there in a positive tone could potentially go a long way. It's tough on the researcher due to a lot of time being applied for very minimal monetary gain. However, this does give that researcher 'street cred'. Listing vulnerabilities reported to CERT on your resume will take you further than listing certifications.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

TG: Yes and no. The world needs to know about these vulnerabilities, but we need to be careful on picking and choosing which vulnerability we will be marketing.

On a regular basis there are vulnerabilities that are rated as a 10 released to the public. Some patched, some not. I think it's great way to spread the word, but I also think it could leave some pretty nasty vulnerabilities to fall to the wayside.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

TG: The NSA was purchasing these zero days in secret previously and may continue to do so. If anything, this just puts the US in a tough spot when competing digitally with other aggressive nation-states, like China.

If the U.S. adheres to the policy change it's possible it could affect the pricing due to a lower demand and plus or minus 25 million dollars a year less being dropped into this underground market. I'm unsure of the actual zero day market share to say whether this is a drop in the bucket or not. We do see costs of zero days ranging from a couple hundred dollars to a couple hundred thousand dollars which is currently significantly more than most bug bounties.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like



HACKED OPINIONS

Hacked Opinions: Vulnerability disclosure - Tomer Schwartz

Adallom's Tomer Schwartz talks about disclosure, bounty programs, and vulnerability marketing



By **Steve Ragan** | Follow

CSO | Jun 29, 2015 4:00 AM PT
Thinkstock



[Adallom's Tomer Schwartz talks about disclosure, bounty programs, and vulnerability marketing with CSO, in the first of a series of topical discussions with industry leaders and experts.](#)

[Hacked Opinions is an ongoing series of Q&As with industry leaders and experts on a number of topics that impact the security community. The first set of discussions focus on disclosure and how pending regulation could impact it. In addition, we asked about marketed vulnerabilities such as Heartbleed and bounty programs, do they make sense?](#)

[CSO encourages everyone to take part in the Hacked Opinions series. If you would like to participate, email Steve Ragan with your answers to the questions presented in this Q&A, or feel free to suggest topics for future consideration.](#)

ALSO ON CSO: The things end users do that drive security teams crazy

Where do you stand: Full Disclosure, Responsible Disclosure, or somewhere in the middle?

Tomer Schwartz (TS), Director of Security Research, Adallom:

In Adallom we always practice responsible disclosure, because as a security company, we understand that some of our responsibility is towards "3rd parties" - users who aren't necessarily a part of our customer base, but nonetheless may be affected by our findings. One of the problems with responsible disclosure is the lack of a formal definition, which allows certain interest groups to take the word "Responsible" and define it in a variety of different ways.

Some vendors believe that the responsible thing to do is to wait indefinitely until a patch is published, but aren't holding themselves accountable for timelines. From my experience, this can be sometimes extend to over a year, without any user being informed, and without any monitoring on whether or not the vulnerability is being exploited in the wild. The majority of security researchers, including myself, find that there is a lack of transparency with this route, and it can be very irresponsible of vendors not to disclose when they know that users are completely vulnerable.

As a security researcher, my opinion is that any choice as to what to do with a vulnerability should be up to the researcher's discretion. Vendors should not coerce researchers either way. Due to bad experience dealing with vendors that are unresponsive and aggressive, some researchers choose not to disclose at all. While I support responsible disclosure, I think it's a terrible state the industry has gotten into.

If a researcher chooses to follow responsible / coordinated disclosure and the vendor goes silent -- or CERT stops responding to them -- is Full Disclosure proper at this point? If not, why not?

TS: Communication is the carrot, full disclosure is the stick. Unresponsive vendors are abundant, and being soft about disclosure deadlines will not make the software industry any better. I think the Zero Day Initiative (ZDI) has done a great job standing behind their position and training the software industry to accept hard deadlines. There are complaints that full disclosures help adversaries, but it's actually the reverse.

Let's consider the scenario of a software vendor that doesn't patch a vulnerability for a year. If the researcher finds this vulnerability and waits to disclose it, someone else might find it and exploit it in that period of time, a whole year in this case - plenty of time for any adversary willing to invest resources in zero-day research. However, if the researcher chooses full disclosure, the same vulnerability will be patched usually in a matter of days. In this case, the period of time users are exposed to the risk is much shorter, even though to them it might look like a scary couple of days.

For the same adversary, the benefit of investing resources on exploiting that unpatched, released vulnerability, decreases dramatically, because she also knows the vulnerability is just about to be patched. While researchers are sometimes crucified in the media for choosing full disclosure, in some cases it is the lesser evil.

Bug Bounty programs are becoming more common, but sometimes the reward being offered is far less than the perceived value of the bug / exploit. What do you think can be done to make it worth the researcher's time and effort to work with a vendor directly?

TS: Bug Bounty programs are a double-edged sword. It is usually a sign for researchers that a company has good understanding of the processes, and are willing to cooperate with researchers.

The monetary incentive also attracts a lot of researchers, which is good for the security of those vendors. On the other hand, that same monetary incentive can also be abused by the vendors to force longer disclosure timelines, and even require the researcher to not go public with the details.

Since it is proportional to the potential value of an adversary, I tend to value a vulnerability or an exploit based on its potential market value in the underground market, and no Bug Bounty program can compete with that today; I doubt any program ever will. Many Bug Bounty programs underestimate the time and efforts required to find a specific vulnerability.

Granted, the researcher disclosing that vulnerability should take it into consideration before disclosure, or even before the research starts. Having said that, the ability to publicly publish an advisory places a unique opportunity for the researcher to build his reputation, which is one of the reasons junior researchers usually do it. This is another reason why I'm against vendors who require the advisory to never be published - it directly harms the researcher.

Do you think vulnerability disclosures with a clear marketing campaign and PR process, such as Heartbleed, POODLE, or Shellshock, have value?

TS: Even though I don't like it at all, I have to acknowledge that it has some value. Without it, the patching cycle for those same vulnerabilities would have been much longer. However, as more and more vulnerabilities are "branded", PR firms are starting to cry wolf and pitch any vulnerability as "the next Heartbleed"; VENOM was a recent example.

Occasionally, critical vulnerabilities are patched without anybody understanding how critical are they, usually because it can take a lot of time to understand the potential impact of a single vulnerability; sometimes longer than the time required to find it in the first place.

The vulnerability branding trend trains the market to differentiate between the "cool", branded vulnerabilities and the old-school CVE-#####; it harms the industry since the latter can sometimes be as important as the former, if not even more. In general, the faster patching cycles are, regardless of media attention, the better.

If the proposed changes pass, how do you think Wassenaar will impact the disclosure process? Will it kill full disclosure with proof-of-concept code, or move researchers away from the public entirely preventing serious issues from seeing the light of day? Or, perhaps, could it see a boom in responsible disclosure out of fear of being on the wrong side of the law?

TS: It's hard to predict what will be the exact terms when (or if) Wassenaar becomes law, and the wording can drastically impact the outcome. Any implementation of a law takes time, and execution is hard, so any change will probably be more gradual than immediate.

The Computer Fraud And Abuse Act (CFAA) is already pretty vague, and was exercised in court in a variety of different ways, so even without Wassenaar passing, some areas of security research are already exposed to legal threats. In the long run, I doubt this type of changes to law will encourage disclosure; in my opinion, it is more likely to increase self-censorship.

Currently it's very hard to estimate the magnitude of this problem, as it's hard to tell how many researchers prefer to keep their names out of their own findings. It's already a complicated situation that Wassenaar is not going to make any easier.



Steve Ragan — *Senior Staff Writer*



Insider: How a good CSO confronts inevitable bad news ➤

 **View Comments**

You Might Like

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3b-yft3
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0159

Comment on FR Doc # 2015-11642

Submitter Information

Name: Cristin Goodwin

Address:

Microsoft Corporation

1 Microsoft Way

Redmond, WA, 98052

Phone: (425) 882-8080

General Comment

Attached are comments provided by Microsoft Corporation on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49).

Attachments

Microsoft - Intrusion Software Submission - BIS-2015-2011 - RIN 0694-AG49

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3b-ci5g
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0160

Comment on FR Doc # 2015-11642

Submitter Information

Name: Tom Cross

Address:

Drawbridge Networks
3423 Piedmont Rd NE
Atlanta, GA, 30305

Email: tom@drawbridgenetworks.com

Organization: Drawbridge Networks

General Comment

See attached file(s)

Attachments

IntrusionCommentsTC

Comments on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Submitted by:

Tom Cross

CTO – Drawbridge Networks

tom@drawbridgenetworks.com

Thank you for opening a public comment period regarding the proposed implementation of export controls on Intrusion items. I am writing because I believe that these regulations may interfere with important work that computer security professionals do to protect the Internet from attacks. Breaches of both government and private sector computer networks are a regular item in the headlines, and they have significant impacts on our economy and our national security. The recently disclosed breach at the Office of Personnel Management that resulted in the loss of security clearance information about millions of Americans is stark example of the problem that we are trying to combat.

The Bureau of Industry and Security (BIS) should exercise caution before taking steps that could make this problem worse than it already is. Export Controls on computer security information can have a chilling effect on important international collaboration, even if that is not intended. Furthermore, it may be difficult to measure the security failures that are the secondary effects of that breakdown in collaboration.

I am qualified to address this topic because I have professional expertise with both US Export Controls and Computer Security Vulnerability Research. From 2003 to 2012 I worked for Internet Security Systems (ISS), which was acquired by IBM in 2006.

At ISS, I served as an engineering advisor to their export compliance program. I helped the company understand how the software we were building fit into the framework of US Export Controls. In collaboration with our attorneys, I wrote Letters of Explanation to BIS for a number of different Export Classifications and I wrote one Commodities Jurisdiction request to the State Department.

Additionally, as part of my job, I engaged in primary computer security vulnerability research and for some time I managed the organization's vulnerability research work. I identified vulnerabilities in popular commercial software applications, disclosed those vulnerabilities to the responsible software vendors, and worked with them to fix those issues. I participated in security industry information sharing programs in which technical information about vulnerabilities, and attack tools, is privately shared between information security companies, coordination centers, and the broader software industry. I had access through those programs to more technical detail about certain security vulnerabilities than was ever disclosed to the general public. It was my responsibility to ensure that ISS's products correctly detected attack activity targeting those vulnerabilities. Those products are used by thousands of organizations around the world to protect their computer networks from attack.

I have broken my comments into four sections:

I. Technical Information about computer security issues that is shared between software vendors, computer security companies, and coordination centers is not necessarily ever disclosed to the public.

BIS has responded to several questions regarding the disclosure of information about vulnerabilities to software vendors and security software companies by explaining that information which is being prepared for public disclosure is not controlled. For example, see the answers to Questions 10 and 19 in the FAQ that BIS published on their website.

It is important for BIS to understand that often, detailed technical information that is provided as a part of a vulnerability disclosure is never shared with the public, that this detailed technical information often includes specific categories of information that BIS says will be controlled under the proposed rule, and that premature public disclosure of this information can and does fuel criminal activity.

I coauthored a paper with a colleague at Microsoft that provides numerous charts showing the timeline of public disclosure of information about different security vulnerabilities, with data about the amount of malicious attack activity targeting those vulnerabilities at different points in time. [1] One need not read our entire paper to get a sense of the impact that public disclosure can have. The first figure in the paper is particularly noteworthy. It comes from a different paper written by researchers at Symantec, [2] and shows the amount of attack activity both before and after disclosure of quite a few different vulnerabilities.

Of course, it is important to disclose some technical details about security vulnerabilities to the public, for the same reason that other kinds of fundamental research are disclosed – to help inform the community of practitioners about the technical facts and enable a discourse to occur about solutions. But, exactly what information to disclose and exactly when to disclose it is often a complex balancing act that is determined on a case by case basis by the specific parties involved in the disclosure. A government policy requiring the public disclosure of certain technical details about vulnerabilities that are being shared across borders will cause the public disclosure of information that otherwise would have been held back, and some of these otherwise unnecessary disclosures will fuel criminal activity.

In answering questions about vulnerability disclosure, BIS has attempted to clarify that technical information about vulnerabilities themselves would not be controlled (Answer to FAQ Question 4). However, the FAQ that BIS published also clarifies that the controls will apply to several categories of information that are important parts of a vulnerability disclosure. In particular, the answer to Question 4 states that “information on how to prepare the exploit for delivery or integrate it into a command and delivery platform” would be controlled. Vulnerability disclosures often include information about how an exploit might be delivered to a target, so that the receiving organization can properly assess the risk associated with the vulnerability and the practicality of an attack.

BIS also states that “technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures” would be controlled. Vulnerability disclosures often include in depth technical explanations regarding how reliable exploitation can be achieved, including how to defeat countermeasures. There are thousands of security vulnerabilities disclosed every year, and people who work to protect networks have to prioritize the work that they do by focusing on the vulnerabilities that pose the highest risk. Questions about the reliability of an attack play a significant role in that prioritization process.

Microsoft is a company that has a particularly mature vulnerability disclosure process, and several aspects of that process provide examples of the way that this sort of information factors into a vulnerability disclosure. Microsoft has an index that they publish along with every vulnerability that they disclose, called the “Microsoft Exploitability Index,” that indicates to the public how likely they believe exploitation of each vulnerability to be. [3] Microsoft states that this index is determined, in part, through an assessment of “the cost and reliability of building a working exploit for the vulnerability, based on a technical analysis of the vulnerability.” That assessment is often informed by detailed technical information provided by the original vulnerability researcher along side the disclosure. That detailed technical information is not always publicly disclosed, and doing so prematurely can help criminals.

Microsoft also has a specific program that rewards vulnerability researchers with bug bounties in exchange for technical information about bypassing protective countermeasures. [4] Under this program, “qualified mitigation bypass submissions are eligible for payment of up to \$100,000 USD.” Technical information about mitigation bypasses is as much a part of vulnerability research as the vulnerabilities themselves.

In addition, BIS wrote in the answer to Question 18 of their FAQ that Exploit Toolkits would be controlled. Security companies often share samples of Exploit Toolkits that are being used by criminals. It is important to test security software against the actual attacks that are happening in the wild, to make certain that those attacks are being correctly detected and blocked by that security software. Prohibiting the sharing of these samples across borders would be extremely disruptive.

BIS’s answers regarding the timing of public disclosure have also been too vague. As the vulnerability disclosure timelines in our paper demonstrate, it can take many months to fix complex vulnerabilities, and longer still for those fixes to be installed broadly enough across the Internet that it becomes relatively safe to publicly disclose detailed technical information about those vulnerabilities without arming attackers by doing so. I’ve personally seen numerous situations where more than a year has elapsed between the initial discovery of a vulnerability and the public disclosure of detailed information about that vulnerability.

During the time window between initial discovery and eventual public disclosure of a vulnerability, that detailed technical information may pass through a lot of hands, including researchers, coordination centers, bug bounty program administrators, employees of the responsible software vendor (who may work in different countries and may be of different nationalities), employees of various

information security software companies (who also may be all over the world), etc. Is all of that detailed technical information clear of export controls during the entire time that the vulnerability is being worked on, just because some day, more than a year in the future, there is a desire to publicly disclose it?

The bottom line is that the proposed rules, as they stand, will be extremely disruptive to computer security research, coordination, and remediation, and will have to be considerably more narrow and precise in order to avoid creating problems.

[1] <https://www.virusbtn.com/files/StewartCross-VB2013.pdf>

[2] https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

[3] <https://technet.microsoft.com/en-us/security/cc998259.aspx>

[4] <https://technet.microsoft.com/en-us/security/dn425049.aspx>

II. The proposed regulation could disrupt the education and development of information security professionals.

One of the primary challenges that we face in protecting computer networks is the small number of truly talented information security professionals available. There are a variety of organizations that offer commercial training classes that play an important role in the development of new information security professionals. These classes often cost thousands of dollars per student for a few days of training. They have small class sizes with a great deal of instructor interaction and lab time.

These classes often teach students how to create controllable, reliable exploits, and how to prepare exploits for delivery, among other things. Every information security professional needs to have some hands on experience with these things, so that they understand exactly what they are and how they work. You simply cannot become proficient at protecting computer networks from attack if you don't understand how to attack them. If you don't understand the realities of exploitation on a first hand basis, you aren't equipped to think about how to interfere with it.

BIS states in the answer to FAQ Question 4 that information about creating reliable exploits and preparing exploits for delivery is controlled "technology." My understanding is that commercial training classes that involve subject matter that is export controlled "technology" cannot be offered to foreign national students. If that understanding is correct, it could have a very disruptive impact on these classes. The teachers and students of these trainings often cross national borders, because there are so few people in the world who are qualified to teach these classes at the highest level. My employer once flew me to Germany for the purpose of taking a class on reverse engineering oriented toward computer security researchers, with a set of students from a diverse set of countries.

It may be necessary for BIS to craft a new public disclosure exception, similar to 734.9, which covers commercial training classes that are not offered in an academic setting.

III. Computer security professionals need to be able to travel outside of the country with their personal laptops and cellular phones without fearing that they may have violated the law by doing so..

The Supplementary Information for the Proposed Rule states, in the context of ECCN 4A005 and 4D004, that “No license exceptions would be available for these items, except certain provisions of License Exception GOV.” Presumably, this means that license exception BAG (740.14) will not be available. There are thousands of people who work in information security who have software on their laptops that would be controlled under the proposed rule, including, for example, commercial penetration testing tools, as well as code that has not been publicly disclosed. If there is no license exception for temporary export of personal items, these people will face prosecution every time they leave the country with their laptops. That is an unreasonable burden to place on all of these people, and it will have no demonstrable human rights benefit. License Exemption BAG should apply to all of these items as well as the associated “technology.”

IV. The Wassenaar approach to controlling “intrusion software” related items is fundamentally flawed. Foreign implementation may harm US interests regardless of how the US decides to implement it.

BIS has issued inconsistent statements about the applicability of the proposed “technology” controls to vulnerability information. The Federal Register states that “Technology for the development of intrusion software includes proprietary research on the vulnerabilities.... of computers and network-capable devices.” However, the answer to Question 4 of the FAQ states that “The proposed rule would not control... Information about the vulnerability, including causes of the vulnerability.” The real truth here is that the answer to this question is not clear, different countries may have different interpretations of the rule, and the consequences are significant.

The US Software industry depends upon the open flow of information about security vulnerabilities, exploitation techniques, and samples of attack tools from security researchers all over the world. If, in trying to implement Wassenaar, other countries prohibit or deter their security researchers from sharing important information with Americans and American companies about security issues, that will create risks for anyone who uses software developed here.

The Wassenaar negotiators should have engaged in broader outreach within in the information security world before reaching an agreement about what controls to put in place. Now that they’ve crafted a rule, I feel that there is a desire in some quarters to come up with a “quick fix” or interpretive approach that will allow the US government to proceed with enforcing it, without any negative consequences. It is not clear to me that this is possible.

I don’t like the idea of US companies providing offensive computer intrusion tools to the militaries, intelligence agencies, and domestic police forces of foreign countries that do not share American principles regarding the right to individual privacy and freedom of speech. However, because of the risk that regulating this

activity poses for information security, if we're going to craft an entirely new set of rules, they should be crafted in the most narrow fashion possible, and then adjusted later if they aren't working in practice.

It's not clear to me that there are significant problems with the diversion of these technologies from civilian to military use. I don't think Governments buy offensive intrusion software frameworks from companies like HackingTeam because they don't know how to make that software themselves and can't figure out how. They buy intrusion software frameworks from software companies for the same reason that they buy word processing software from software companies, because it's cheaper and more expedient to buy off the shelf products than it is to develop something from scratch on your own, even if you know how.

Therefore, I think that a rule which narrowly controlled the commercial sale of intrusion software frameworks that are "specially designed" for a military, intelligence, or police end use and specifically marketed to those end users might be sufficient to address the human rights concern that is being raised here, without impacting any legitimate defensive computer security work. Unfortunately, that is not what Wassenaar agreed to.

Thank you for taking the time to read and consider my input on this important matter. Feel free to email me if you have questions or desire further clarification about any of the points that I have made herein.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-4vom
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0161

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

This is, what we in the information security industry call, "a bad idea".

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-ead1
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0162

Comment on FR Doc # 2015-11642

Submitter Information

Name: Sam Houston

Address:

2678 21st st

San Francisco, CA, 94110

Email: sam@qforq.com

Organization: Bugcrowd

General Comment

Hello,

I work for a company that helps make our customers more secure through the help of security researchers. We work with over 18,000 security researchers from all over the world, a community of people that "hack" on our customers and find security issues in their products. We work with some of the biggest companies in the world, including Western Union, Tesla and Pinterest.

This new implementation would make our jobs much harder, and in some cases, would inhibit our ability to work with world-class talent that find security vulnerabilities in our customers' products. We would be severely impacted, unable to take vulnerability submissions from our overseas workers in some cases.

I ask that you please reconsider this implementation and work with the security community to create legislation that actually makes everyone safer, both by limiting proper things but also allowing work done by the security researcher community.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-m6t3
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0163

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nathaniel Vos

Address:

1510 Heathfield Dr NE
Grand Rapids, MI, 49505

Email: maniac_4jc@hotmail.com

Phone: 616-855-0945

General Comment

While the rules here are well-intentioned, the skills and expertise to discover, write exploits, and comment on architectural secrets are widely distributed throughout the world. Placing export controls on Americans working on demonstrating a software flaw or publishing a bug endanger all of us. We rely, as a community, on people being able to freely investigate and publish the weaknesses they find as soon as possible, so we can mitigate damages. In addition to that harm, much of this activity will just migrate to other parts of the world.

A swift response to a bug relies on quick world wide dissemination to allow professionals to test their software, patch their networks, etc. Hampering this process impedes all of this positive defensive activity, and provides no deterrent to the seething hordes of hackers and miscreants throughout the world, who I assure you, have no interest in abiding by export controls.

Tools are just that tools. They can be used for good or ill, and the regulations here prevent (or at least hinder) their positive uses and development, while encouraging negative outcomes (in the sense that, if no one is working on fortifying the locks, the thieves have a much better chance of picking them). Remember, a tool like metasploit allows IT pros to systematically test and secure

their networks. Removing a tool like that does not remove the underlying flaws, just makes it that much more difficult to find and remove them! How is that helpful?

Perhaps a better path forward will be to place stronger liability on companies that release insecure products, and not to punish those who try to improve the security situation after the fact.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-d8bk
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0164

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jacob Brodsky

Address:

1371 Woodbine Road
Woodbine, MD, 21797

Email: ab3a@verizon.net

Phone: 4104892898

General Comment

While the intents of the Wassenaar Arrangement are noble, the execution and the management are such that it can only lead to tyranny. In fact, such methods conflict with our own Bill of Rights enshrined in the Constitution.

First, there is the problem with free speech. Writing books about encryption, and publishing software that can perform encryption is not against the law and can not be against the law despite many efforts to do so. No government in the US, particularly a Bureau of the Federal Government, can legitimately squelch such efforts. The BIS has no legal basis for legislating what a person can say, even if it is encrypted.

So instead, through international agreements which have not and likely never will be ratified by the Senate, BIS seeks to define encryption as a munition. Is it a munition? I suppose it could be viewed that way. It is in fact a defensive measure commonly used by many security conscious professionals to protect their data at rest, and to conduct commerce confidentially. Nevertheless, there is a Second Amendment which guarantees the right to keep and bear arms. Classifying this technology as a munition does not make a case for regulation. The last time I checked, the

Second Amendment is still the law of the land. The BIS has to build a much stronger case for licensing a primarily defensive technology back to the citizens of this country. Merely claiming that this is in alignment with an unratified treaty is insufficient.

Legal theories aside, there is no practical way to license this technology. Those who want it already have it. Those who seek it can find it anywhere. Regulating what people read or download is not something that BIS or any government agency can practically manage.

Furthermore, regulating against software penetration and testing tools will simply move the technology to another country that did not sign the Wassenaar Arrangement. These technologies will continue to spread on the Internet, only this time, because of BIS bureaucracy, the law abiding citizens who need such technology won't have it.

Frankly, this headlong effort to align with the Wassenaar Arrangement is fraught with so many practical and legal problems that I think these regulations are counterproductive and onerous. I strongly recommend dropping this proposed rule.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-5c3w
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0165

Comment on FR Doc # 2015-11642

Submitter Information

Name: Robert Graham'

Address:

GA,

Email: robert_david_graham@yahoo.com

General Comment

Hi.

I created the first intrusion prevention system, as well as many tools and much cybersecurity research over the last 20 years. I would not have done so had these rules been in place. The cost and dangers would have been too high. If you do not roll back the existing language, I will be forced to do something else.

After two months, reading your FAQ, consulting with lawyers and export experts, the cybersecurity industry still hasn't figured out precisely what your rules mean. The language is so open-ended that it appears to control everything. My latest project is a simple DNS server, a piece of software wholly unrelated to cybersecurity. Yet, since hackers exploit DNS for malware command-and-control, it appears to be covered by your rules. It's specifically designed for both the distribution and control of malware. This isn't my intent, it's just a consequence of how DNS works. I haven't decided whether to make this tool open-source yet, so therefore traveling to foreign countries with the code on my laptop appears to be a felony violation of export controls.

Of course you don't intend to criminalize this behavior, but that isn't the point. The point is that

the rules are so vague that they become impossible for anybody to know exactly what is prohibited. We therefore have to take the conservative approach. As we've seen with other vague laws, such as the CFAA, enforcement is arbitrary and discriminatory. None of us would have believed that downloading files published on a public website would be illegal until a member of community was convicted under the CFAA for doing it. None of us wants to be a similar test case for export controls. The current BIS rules are so open-ended that they would have a powerful chilling effect on our industry.

The solution, though, isn't to clarify the rules, but to roll them back. You can't clarify the difference between good/bad software because there is no difference between offensive and defensive tools -- just the people who use them. The best way to secure your network is to attack it yourself. For example, my masscan tool quickly scans large networks for vulnerabilities like Heartbleed. Defenders use it to quickly find vulnerable systems, to patch them. But hackers also use my tool to find vulnerable systems to hack them. There is no solution that stops bad governments from buying intrusion or surveillance software that doesn't also stop their victims from buying software to protect themselves. Export controls on offensive software means export controls on defensive software. Export controls mean the Sudanese and Ethiopian people can no longer defend themselves from their own governments.

Wassenaar was intended to stop proliferation and destabilization, yet intrusion/surveillance software is neither of those. Human rights activists have hijacked the arrangement for their own purposes. This is a good purpose, of course, since these regimes are evil. It's just that Wassenaar is the wrong way to do this, with a disproportionate impact on legitimate industry, while at the same time, hurting the very people it's designed to help. Likewise, your own interpretation of Wassenaar seems to have been hijacked by the intelligence community in the United States for their own purposes to control Odays.

Rather than the current open-end and vague interpretation of the Wassenaar changes, you must do the opposite, and create the narrowest of interpretations. Better yet, you need to go back and renegotiate the rules with the other Wassenaar members, as software is not a legitimate target of Wassenaar control. Computer code is not a weapon, if you make it one, then you'll destroy America's standing in the world. On a personal note, if you don't drastically narrow this, my research and development will change. Either I will stay in this country and do something else, or I will move out of this country (despite being a fervent patriot).

Robert Graham
Creator of BlackICE, sidejacking, and masscan.
Frequent speaker at cybersecurity conferences.
robert_david_graham@yahoo.com
@ErrataRob

Attachments

bis-comment

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3c-5ioh
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0166

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

As a security professional trying to help protect critical systems and application I fear this law will have adverse affects to my work, research and tool development.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3d-v6qo
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0167

Comment on FR Doc # 2015-11642

Submitter Information

Name: Dave Weinstein

General Comment

Others have addressed the chilling impact that the proposed regulations would have on independent security researchers. I'd like to address the impact that they would have on the development of software in general, and more specifically how they would impair the ability of software development companies to produce secure software products.

There is a general shortage of skilled programmers in almost all parts of software development. This shortage becomes acute when looking for security specialists. Partly this is because of the relative scarcity of security specialists as a whole, and partly this is because most of the security specialists available do not have experience in developing general purpose software.

This is not in and of itself unreasonable; after all, we'd prefer the engineers building our aircraft control systems be experts first and foremost in avionics, the engineers building medical equipment to be experts in medical technology, and even the engineers building our email systems to experts in delivering our mail in a timely fashion. What this means is that the security specialists in software development are often working with multiple teams, and are often not developing the core of the software themselves, but rather are working with the teams to make that software secure.

What becomes problematic is the notion of "deemed export". Software is often developed across multiple countries, and even if in the same country, is often developed with developers who are foreign nationals.

So, let's consider a very real case, and one I've personally seen as both a software developer and as a security researcher. A product is nearing its scheduled ship date, and a security specialist has found a problem which needs to be fixed, even if it means delay. Even with the best intentions, it is not unreasonable for a development manager to insist on proof that the risk is real before a delay. At this point, even a simple proof of a software defect may not be sufficient, and the security analyst may have to write a complete exploit.

At this point, we have a case where the engineer responsible for the vulnerable feature may not be allowed to look at the full details of the problem. The manager who would have to argue the case up the line may not be allowed to know exactly what went wrong. The executive responsible for making the final call may not be able to be shown the ramifications of a decision to ship anyway.

"Deemed export" and other limitations on transfers of information within the same company are not going to make us any safer from criminals or hostile nation states. But what they may do is make it harder for us to produce software that is more resilient against attack.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3d-f1sj
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0168

Comment on FR Doc # 2015-11642

Submitter Information

Name: John Anderson

General Comment

Security research must protected under the law. Hackers who are skilled enough to break into software and networks but choose to share their knowledge should be legally exempt from criminal prosecution. The war being fought for security and privacy on the Internet needs all hands on deck when it comes to defense. Hackers should find the path of least resistance to help defenders; they should not run into trouble with the law when trying to help.

Rather than the current vague interpretation of Wassenaar changes, you must do the opposite and create the narrowest of interpretations. Better yet, you need to go back and renegotiate the rules with other Wassenaar members, as software is not a legitimate target of Wassenaar control. Computer code is not a weapon, if you make it one, Americas standing in the world will be diminished.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3d-pngp
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0169

Comment on FR Doc # 2015-11642

Submitter Information

Name: Dave Lewis

Address:

2255B Queen Street East

Suite 156

Toronto, Ontario, Canada, M4E 1G3

Email: dave@liquidmatrix.org

Phone: 416-619-9091

Organization: Liquidmatrix Security Digest

General Comment

I want to take a moment to comment on the proposed rules. I believe that these rules as currently written will have an unintended negative impact on the field of security research overall. We need to be cognizant that restrictive rules applied to security research will only improve the odds for negative elements who would not feel any obligation to comply. In order to mount a proper defence in the digital world we need to be able to have a clear and open dialogue on security subjects. If there is embarrassment to be experienced by software companies this would be a necessity to better secure the wider audience.

The rules should have a great level of clarity applied to limit confusion and misinterpretation. While I understand the spirit and intent, I feel rather strongly that clarity needs to be sharpened and that the proposed rules are revisited before being put into practice.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3d-y1oo
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0170

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Although this regulation will probably provide some powerful new legal and operational tools to some parties belonging to some scopes (military, intelligence, mostly), most probably will result at some point not too far in the future in effectively crippling many internal infrastructures, given the lack of cooperation of foreign actors, a natural consequence of the imposed non-cooperative policy.

That cost / benefit relationship should be carefully analyzed, any biased analysis could be dangerous.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-48o9
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0171

Comment on FR Doc # 2015-11642

Submitter Information

Name: Adam Pridgen

Address:

180 Spyglass Park Lane
Montgomery, TX, 77316

Email: adam.pridgen@thecoverofnight.com

Phone: 2104467805

General Comment

I'm a penetration tester and someone who works in security who develops tools and/or exploits, in addition to using tools and exploits developed by other researchers in the community. I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-ezo3
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0172

Comment on FR Doc # 2015-11642

Submitter Information

Name: Mara Tam

General Comment

See attached file(s)

Attachments

comments_BIS-2015-0011

BIS-2015-0011-0001, Wassenaar Arrangement 2013 Plenary Agreements
Implementation : Intrusion and Surveillance Items

To Kevin Wolf, Assistant Secretary for Export Administration, and to Randy Wheeler, Director of the Information Technology Controls Division of NSTTC,

Thank you for opening this period of public comment on the proposed 'cyber rule'. Though there are numerous, severe obstacles to achieving a clear and effective final rule, I have been consistently impressed with BIS' dedication to and eagerness to learn from the affected community. However, I must advise that, following a review of these and other public comments, BIS move to publish a second proposed rule and open a second, 60-day period of public comment. We are out of time, and, though the gulf between practitioners and regulators has narrowed considerably since the proposed rule's publication, there is still much work we must do together in order to reach our common goals.

This work has been made all the more difficult by a separate proposed rule to revise both the core definitions of the EAR as part of the Administration's Export Control Reform Initiative (ECRI). [^"Revisions to Definitions in the Export Administration Regulations; Proposed rule with request for comments," 80 FR 106 (3 June 2015), pp.31505-20.] This proposed rule also contains amendments to the Scope section of the EAR which, along with many of the revised definitions, contribute even more uncertainty to the implementation of this proposed 'cyber rule'. [^§734.7 – 'Published Technology and Software', §734.8 – 'Fundamental Research', new §734.13 – 'Export', new §734.14 – 'Reexport', new §734.16 – 'Transfer (In-Country)', new §734.17 – 'Export of Encryption Source Code and Object Source Code Software', new §734.18 – 'Activities That Are Not Exports, Reexports, or Transfers', new §734.20 – 'Activities That Are Not Deemed Reexports', §772.1 – 'Technology', and further elements of this proposed rule introduce enough potential variance in application as to make clear assessment of the proposed 'cyber rule' by the affected population impossible at this time.]

These comments provide cursory background on the advocacy for and introduction of these technologies into the Wassenaar Arrangement (WA), a similarly brief discussion of problems with the proposed rule inherited by BIS from WA, and a more targeted analysis of particularly problematic language within in the proposed rule. Unintended consequences of the proposed rule for national security and foreign policy are addressed and specific proposals made throughout.

Background : the 'human rights nexus' _

As Ms Wheeler noted during the weekly ECR teleconference held on 20th May 2015, BIS was made aware of a 'human rights nexus' to the intrusion and surveillance items currently under discussion. While implementation of new Wassenaar Arrangement provisions is non-negotiable, understanding their purpose and relative efficacy remains an essential part of the rule-making process. In the case of this proposed rule, its intended and actual consequences are, at the time of writing, unacceptably divergent.

Though the campaign to bring intrusion and surveillance items under export control through the Wassenaar Arrangement predates the events of the Arab Spring, 2011 saw the movement dramatically expand in both participation and profile. Revelations regarding the use of sophisticated surveillance software against activists and dissidents in Syria, [^Jennifer Valenti no-Devries, Paul Sonne and Nour Malas, 'U.S. Firm Acknowledges Syria Uses Its Gear To Block Web,' *The Wall Street Journal*, 29 October 2011. <http://www.wsj.com/articles/SB10001424052970203687504577001911398596328>], [^Behind Blue Coat : Commercial Filtering in Syrian and Burma,' *The Citizen Lab* Research Brief (November 2011). <https://citizenlab.org/wp-content/uploads/2015/03/Behind-Blue-Coat-Investigations-of>

-Commercial-Filtering-in-Syria-and-Burma.pdf], [^Morgan Marquis-Boire and Seth Hardy, 'Syrian Activists Targeted with BlackShades Spy Software,' *The Citizen Lab* Research Brief (June 2012). <https://citizenlab.org/wp-content/uploads/2015/03/Syrian-Activists-Targeted-with-BlackShades-Spy-Software.pdf>], Egypt, [^Karen McVeigh, 'British firm offered spying software to Egyptian regime – documents,' *The Guardian*, 28 April 2011. <http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-fisher>] Morocco, [^Ryan Gallagher, 'How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists,' *Slate*, 20 August 2012. http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_websi_te_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html] Bahrain, [^Morgan Marquis-Boire, 'From Bahrain with Love: FinFisher's Spy Kit Exposed?,' *The Citizen Lab* Research Brief (July 2012). <https://citizenlab.org/wp-content/uploads/2015/03/From-Bahrain-With-Love-FinFishers-Spy-Kit-Exposed.pdf>] and elsewhere, [^Morgan Marquis-Boire, 'Backdoors are Forever: Hacking Team and the Targeting of Dissent,' *The Citizen Lab* Research Brief (October 2012). https://citizenlab.org/wp-content/uploads/2015/03/Backdoors-are-Forever-Hacking-Team-and-the-Targeting-of-Dissent_websitepdf.pdf] raised the politically uncomfortable prospect of European and American technologies being deployed in the service of oppressive regimes around the world. Clearly, something needed to be done.

Dutch Member of European Parliament Marietje Schaake has been agitating for the regulation of surveillance technologies since at least 2010, and remains the MEP most prominently involved in pursuing action to stem the proliferation of surveillance technologies. [^<http://www.marietjeschaake.eu/2010/10/parliamentary-question-eu-policy-on-regulation-of-surveillance-technology/>] In the United States, Christopher Soghoian has been a similarly prominent voice in the campaign against state surveillance, both in his role as Chief Technologist for the American Civil Liberties Union (ACLU), and from 2009 until he commenced employment with ACLU in 2012.

By the beginning of 2013, regular media coverage and technical reports from *The Citizen Lab* were joined by calls for the offending technologies to be more heavily regulated. While EU and US sanctions targeting Syria and Iran imposed some limits on the export of intrusion and surveillance technologies, by the end of 2011 a growing number of voices declared these measures grossly inefficient and advocacy began to shift towards regulation of the industry en bloc. [^<https://advocacy.globalvoicesonline.org/2011/11/15/us-and-european-firms-help-syrian-regime-spy-on-citizens/>], [^<http://consentofthenetworked.com/2011/11/01/surveillance-technologies-and-political-corporations/>] London-based Privacy International (PI) was a prominent, early voice advocating for new export controls.

With strong support from human rights and privacy advocates on both sides of the Atlantic, the 2013 Plenary Session of the Wassenaar Arrangement introduced new intrusion and surveillance entries to be controlled under the dual-use regime. [^] As written, these controls present significant challenges in implementation, and these problems may soon be compounded by ongoing, misguided advocacy.

In April 2014, the Coalition Against Unlawful Surveillance Exports (CAUSE) was officially launched with PI as its secretariat. [^] In addition to PI, the membership of CAUSE is comprised of Access, [^<https://www.accessnow.org/>] Human Rights Watch (HRW), [^<http://www.hrw.org/>] Digital Gesellschaft, [^<https://digitalgesellschaft.de/>] La Fédération internationale des ligues des droits de l'Homme (FIDH), [^<https://www.fidh.org/Surveillance>] Amnesty International, [^<https://www.amnesty.org/en/>] Reporters Without Borders (RSF), [^<http://en.rsf.org/>] and the New America Foundation's Open Technology Institute (OTI). [^<http://www.newamerica.org/oti/>] The most recent statement from this group calls on the EU to implement even broader controls on intrusion and surveillance technologies than those adopted through the WA in December 2013, and recommends that new technologies and equipment identified by the review of the Dual

Use Regulation be subsequently introduced to WA. [^A critical opportunity : bringing surveillance technologies within the EU Dual-Use Regulation, ' *CAUSE* policy document (June 2015). <https://privacyinternational.org/sites/default/files/CAUSE%20report%20v7.pdf>]

Paved with good intentions

The addition of new intrusion and surveillance technology entries to WA during the December 2013 Plenary Session was motivated by concern over the deployment of these technologies by oppressive regimes. However, the efficacy of a top-down approach to mitigating the potential harm of these technologies in the hands of state surveillance organs must be called into question. Not even the most sophisticated commercial products from among the offerings of these firms is capable of creating a surveillance capability where none existed before. Through Hacking Team's recently compromised documentation, it has become more and more evident that these products often rely on physical access to target devices, and most reliably provide a friendlier user interface for state security organs.

These statements should not be mistaken as a defence of surveillance and intrusion technologies deployed by a government against its citizenry, but should bring into focus the moral argument against them. In much the same way that encryption does not make surveillance impossible, but may make it more difficult, these technologies do not make surveillance possible, but they may make it easier. Even in high-quality technical reports such as those produced by *The Citizen Lab*, it remains extremely difficult to assess the risk posed to targets of these technologies compared with the baseline of their respective governments' surveillance capabilities and observed activities. In short, the threat models of non-hypothetical dissident and non-dissident citizens of the regimes known to have employed these commercial surveillance solutions remain ill-defined.

We are not confronted with a choice to permit the non-democratic regimes of the world to surveil. The Bahrains, Ethiopias, and Sudans have already compromised any communications infrastructure - nationalised or private - of interest to their security services. Making surveillance more difficult in cases where it is clear that human rights abuses are taking place should be a foreign policy priority for the United States, but the solution offered by WA in its current form has already, with Hacking Team's shocking and legal circumvention of its implementation in Italy, proven itself to be ineffectual. [^<https://wikileaks.org/hackngteam/emails/emailid/174537>], [^<https://www.wikileaks.org/hackngteam/emails/emailid/158220>] BIS' proposed implementation carries with it all of the shortcomings of the WA language as well as a number of unique risks to U.S. national security, foreign policy, and to the global task of information security.

Unintended consequences

As written, the proposed rule contains several severe risks to national security, but perhaps the most severe among them comes from §742.6(b)(5) *Licensing policy for cybersecurity items*. Imposing a licensing requirement on the new cybersecurity items for all destinations except Canada is certain to cripple coordinated defence and threat-sharing information within global supply chains vital to U.S. national security. Information security researchers must be able to defend unfettered and unafraid; the present rule presents unacceptable obstacles to that goal.

Proposal s

1. Draft a second proposed rule and open a second period of public comment.
2. Introduction of broad, multi-year licenses for controlled items.
3. Explicit license exemption for vulnerability reporting.

4. §742.6(b)(5) *Licensing policy for cybersecurity items* states that 'there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.' [^"Wassenaar Arrangement 2013 Plenary Agreements Implementation:

Intrusion and Surveillance Items; Proposed rule with request for comments," 80 FR 97 (20 May 2015), p. 28858.] This language cannot be present in a final rule. BIS' statements on their understanding of the terms 'rootkit' and 'zero-day exploit' indicate profoundly deficient guidance on the defensive uses of offensive technologies (e.g. deployment of rootkit-based technologies for endpoint protection). Current and next-generation defence not only incorporate technologies traditionally considered to be 'offensive', they rely on them.

BIS has stated that they understand the presence or support of rootkit / zero-day exploits to indicate that a product is 'offensive by design'. To maintain this understanding as a basis for regulation would be to regulate on the basis of a specious respectability politics devoid of technical merit.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-9mfo
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0173

Comment on FR Doc # 2015-11642

Submitter Information

Name: Amir Etemadieh

Address:

2001 Harvest Moon Dr
Cedar Park, TX, 78613

Email: Zenofex@Exploitee.rs

Phone: (512)981-7668

Organization: Exploitee.rs

General Comment

See attached file(s)

Attachments

Exploitee.rsWassenaarComment

We (The Exploiters) are a group of scientists who research and disclose vulnerabilities within consumer electronic devices. We purchase electronics, then work through reverse engineering the software and hardware of those devices searching for critical flaws that could be leveraged by a malicious attacker. This process requires multiple tools, some Open Source while some not, and generally results in a form of “proof of concept” code being created. This “proof of concept” code allows engineers the ability to initially diagnose the issue through replication of the bug in a test environment as well as test their modifications in the corrected version(s) of their software. The current proposed state of the Wassenaar Arrangement (WA) and its inclusion as well as broad wording of “Intrusion Software” within its definition, however, would prevent security researchers from having the ability to properly provide the needed materials to the hardware or software creators. This type of situation can also put consumers as well as our nation’s corporate structure at risk. By preventing researchers and groups, such as the Exploiters, the ability to freely distribute proof of concept code to the appropriate developers, the WA will cause an unnecessary increase in the time it takes to fix a vulnerability, one that may already be being exploited maliciously.

We also believe that the broad wording in the definition of “Intrusion Software” negatively affects vulnerability research within company sponsored “Bug Bounty” programs by which a researcher is rewarded with either public acknowledgement or an item of value in return for privately disclosing a vulnerability to a vendor. The process consists of a project scope being announced which describes what is allowed and what is rewarded for each finding. A researcher then goes about finding vulnerabilities in the areas allowed, and then discloses the reproduction instructions to the vendor, allowing developers the ability to debug and fix the reported vulnerability. After the developers complete fixing and publishing the newly updated software, the researcher is rewarded for the finding. Such programs allow researchers the ability to help companies fix issues within their software as well as help educate developers on what unintended consequences, such as creating exploitable vulnerabilities, their mistakes can have.

This process has several parts that are affected by the current definition of “Intrusion Software” within the WA. The first of which is the code given to the software creators to replicate and diagnose the vulnerability. This is an integral part of the process and is directly impacted by the portion of the “Intrusion Software” definition which states that intrusion software includes “...software specially designed for the generation, operation or delivery of, or communication with, intrusion software...”. The replication instructions consist of the exact code needed for the vulnerability to occur and therefore will be considered as intrusion software under the WA. The second portion of the bug bounty process in the example above impacted by the proposed definition of “Intrusion Software” is the usage of tools such as “Burp Suite” (BS), a proprietary program that charges a fee for its use but allows researchers and developers the ability to find bugs by passively testing application functionality. The process of using BS involves running the software as a proxy through the tester’s browser while BS actively investigates and manipulates traffic looking for errors in the response that can be indicative of critical vulnerabilities. This tool is essential to any web application tester’s toolset and its use and sale would be heavily regulated through the proposed changes.

The newly proposed definition of “Intrusion Software” will also hinder the security of consumers on a global scale by preventing researchers the ability to create exploit mitigations, or operating system software changes that effectively prevent a wide range of exploits. This is done by identifying a critical portion of the exploitation process and then using that knowledge to add protection to mainstream operating systems. This process has made exploitation increasingly difficult to date but due to proposed changes in the WA, the process may be effectively destroyed because the proposed regulation of exploit code would prevent researchers from sharing attacks and code that may be in the wild but not yet fixed by developers.

In short, the broad wording in the newly proposed changes to the WA is a danger to the Internet as it hinders security research and creates a situation where those that wish to secure their software will be forced to use regulated tools that put them (and as such their employers) at a disadvantage against attackers. We (The Exploiters) therefore request that the current proposed changes to the WA be modified to correctly address the original intention of the WA and after such another comment period held to evaluate the impact of the new definition on security research.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-yj4h
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0174

Comment on FR Doc # 2015-11642

Submitter Information

Name: Joseph FitzPatrick

Email: joefitz@securinghardware.com

Organization: <http://securinghardware.com>

General Comment

The primary focus of my business is hardware security training. While my niche is unique within the training portion of the information security industry, the current wording and intention of BIS's implementation of the Wassenaar Arrangement 2013 Plenary Agreements has the potential to shut down my business and increase the already large knowledge gap in the overall industry.

My training is geared towards information security professionals. In the past year, they have included architects, developers, and validators of computer software and hardware, forensic experts seeking deeper hardware understanding to enable law enforcement, security consultants and penetration testers from most of the leading security consultancies who need hardware background to enable them to do a more thorough job of testing the security of the world's tools and infrastructure, and finally members of the intelligence community who need to understand the state of the art for both defensive and offensive aspects of national security.

Fundamentally, I teach people with varied employers, nationalities, and motivations how to break hardware security. This is the single most effective method to educate the industry how to test the security of current devices and architect the security of the next generation of computing equipment.

The loose wording and ambiguity of BIS's implementation makes it altogether unclear for me to know what, if any license I need in order to continue teaching the skills I teach, without gambling my entire business in the hopes the 'no you don't need a license for that' response I might get when applying for a license is the same interpretation that is rendered when I might be prosecuted for intangible technology transfer.

I am not an academic institution, and I do not publish my training freely, so i do not fit into either of those carved out exceptions. I teach skills to an industry with a huge skills gap. There is effectively 0% unemployment in information security. Technical professional education is my best solution to this problem, and my many customers seem to agree.

The current BIS implementation would be either overbearing in business overhead, or too risky to continue my current business with out risk of violations, resulting in a loss for the security industry and the security of our internet and infrastructure.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-yngk
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0175

Comment on FR Doc # 2015-11642

Submitter Information

Name: Christopher Eng

Address:

285 Bedford St

Lexington, MA, 02420

Email: chris.j.eng@gmail.com

Phone: 339-674-2828

Organization: n/a

General Comment

To Whom It May Concern:

I am a cybersecurity professional with nearly two decades of experience in the field across both the public and private sector. Despite its good intentions, the proposed implementation of the Wassenaar rules as applicable to intrusion software would be damaging to the cybersecurity industry and ultimately the security posture of the US government and American corporations.

In cybersecurity, offense and defense are inextricably linked. In order to effectively defend our infrastructure and the complex software that runs atop that infrastructure, its necessary to understand how they would be attacked. This is what security researchers do. We find creative techniques to exploit security weaknesses in various technologies, then we collaborate on ways to make them safer. Restricting attack-oriented research necessarily inhibits defensive innovations.

Security practitioners regularly collaborate with peers in all corners of the globe, sharing ideas

as well as code. The Internet has made the world a much smaller place, and yet this does not mean viable collaborators are plentiful. Cybersecurity is an umbrella term encompassing hundreds of specialized disciplines, and often the experts with whom you have trusted working relationships reside outside US borders.

In my current role leading security research at Veracode, my team is international. Our company is international. We have employees in Japan, Australia, Israel, and other far-flung regions, and we collaborate daily on vulnerabilities and exploitation of computers. In fact, any company of reasonable size that either develops or uses security tools (i.e. any company with an interest in protecting its customers and its intellectual property) will be negatively impacted by these regulations.

Please do not slow down innovation in cybersecurity research at a time when we need that innovation the most.

Sincerely,
Chris Eng

Attachments

eng-wassenaar

To Whom It May Concern:

I am a cybersecurity professional with nearly two decades of experience in the field across both the public and private sector. Despite its good intentions, the proposed implementation of the Wassenaar rules as applicable to “intrusion software” would be damaging to the cybersecurity industry and ultimately the security posture of the US government and American corporations.

In cybersecurity, offense and defense are inextricably linked. In order to effectively defend our infrastructure and the complex software that runs atop that infrastructure, it’s necessary to understand how they would be attacked. This is what security researchers do. We find creative techniques to exploit security weaknesses in various technologies, then we collaborate on ways to make them safer. Restricting attack-oriented research necessarily inhibits defensive innovations.

Security practitioners regularly collaborate with peers in all corners of the globe, sharing ideas as well as code. The Internet has made the world a much smaller place, and yet this does not mean viable collaborators are plentiful. Cybersecurity is an umbrella term encompassing hundreds of specialized disciplines, and often the experts with whom you have trusted working relationships reside outside US borders.

In my current role leading security research at Veracode, my team is international. Our company is international. We have employees in Japan, Australia, Israel, and other far-flung regions, and we collaborate daily on “vulnerabilities and exploitation of computers”. In fact, any company of reasonable size that either develops or uses security tools (i.e. any company with an interest in protecting its customers and its intellectual property) will be negatively impacted by these regulations.

Please do not slow down innovation in cybersecurity research at a time when we need that innovation the most.

Sincerely,

Chris Eng

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-hk0v
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0176

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael Ossmann

Address:

Great Scott Gadgets
27902 Meadow Dr. Suite 150
Evergreen, CO, 80439

Email: mike@ossmann.com

General Comment

Thank you for inviting comments on the Wassenaar Arrangement Plenary Agreements Implementation for Intrusion and Surveillance Items. As a member of the information security community, I am concerned about the effects of the proposed implementation on my industry.

I'll keep this brief by voicing support for the comments made by other prominent members of the community: Google, Katie Moussouris, Robert Graham, and Sergey Bratus et al.

My greatest concern is clarity of the proposed rule. If you must provide an answer to a frequently asked question about what a rule means, it may be because the rule was not written clearly. I was particularly troubled by the publication of the FAQ regarding the proposed rule, partly because it indicated a lack of clarity in the rule but also because the answers didn't seem much clearer. Had the answers been clear, I would still be concerned that the text of the rule would not be interpreted in the future in the same manner as your present interpretation. The text matters, and it is overbroad and unclear even to well informed members of the information security community.

Unfortunately, computer security is an unsolved problem. The people who are working to improve the state of the art of computer security are diverse members of a global community of researchers. The proposed rule directly prevents the sharing of information among those researchers, and it will have a negative impact on the security of computing systems and software for the entire world.

Software is a form of information, and control of the flow of information is very different from control of the transport of physical goods. I urge you to remove software from the scope of the Wassenaar Arrangement at the annual meeting of Wassenaar Arrangement members in December 2015.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-2cqj
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0177

Comment on FR Doc # 2015-11642

Submitter Information

Name: Tony Webster

General Comment

As a software engineer and security researcher, I'm very concerned with the vagueness of the proposed rules, and the harmful impact these rules would have on broad societal interests in online security.

Bugs in systems and software that could or would be exploited by those who wish to cause malicious or financial harm are routinely first discovered and exploited by vulnerability researchers determined to report and see those flaws fixed before they could be exploited for evil.

Many of these good-intentioned researchers are based in the United States, working for or otherwise reporting these vulnerabilities to companies within the United States but far more are outside of the United States, are U.S. employees that travel overseas, are foreign nationals employed by U.S. companies, or companies working on behalf of a U.S. company. In these situations, vulnerability research intended to better-secure systems that Americans rely on would be halted or delayed, security would be degraded, and our online lives would be much less secure.

Information sharing is of extreme importance to the furtherance of online security in a world where commerce happens worldwide, and these proposed rules would only serve to harm that.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-wb9a
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0178

Comment on FR Doc # 2015-11642

Submitter Information

Name: Adam Caudill

Address:

TN,

Email: adam@adamcaudill.com

Phone: 4238337678

General Comment

The importance of security research is undeniable research that protects people and businesses in the US and around the world. Without the dedication of researchers around the world, this research simply wouldnt happen these regulations, by a combination of vagueness and misunderstanding, of how research is performed, could substantially chill vital research.

Communication is vital to effective research from reporting issues to vendors across borders, bug bounty programs that pay researchers for vulnerabilities and exploits, coordinating with other researchers to identify vulnerabilities and developing exploits needed to validate the effect and severity of the vulnerability, to coordinating disclosure (which may involve working with many parties in different countries to confirm and correct issues) without free communication, many of these activities couldnt happen. While statements have been issued that state some notifications and coordination are not covered by these regulations as worded, that isnt clear and seems subject to later reinterpretation that could greatly expand the impact of these regulations.

Legitimate research should be explicit protected, not left as a vague interpretation detail; without doing so, these regulations will add a great deal of uncertainty for researchers. If a

researcher feels the need to contact an arms control expert before reporting a vulnerability the number of issues being fixed will drop, leading to greater exposure for everyone.

The tools needed to test systems, the details of new research, information in or to be released to the public domain, as with legitimate security research should be explicitly protected; clear, unquestionable, undeniable protection should be added to these regulations to ensure that there isnt a question of interpretation as there is now.

While I understand that a great deal of effort has been put into this implementation, it is an area full of subtleties, subtleties that are not found in other areas. To ensure the safety of people around the world, a great deal of care needs to be taken give the security community the freedom and flexibility necessary to perform the research that is so vital to everyone.

Finally, I strongly recommend that following the review of the comments of this proposed regulation, another round of public feedback be performed. This is a very important area, and has caused a great deal of concern in the security community. More time is needed to help evolve these regulations into something that meets the requirements of the applicable treaties and protects the security community and allows the vital research conducted around the world to continue in an effective manner.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-p4ng
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0179

Comment on FR Doc # 2015-11642

Submitter Information

Name: Karl Koscher

Address:

4174 3rd Ave Apt 27

San Diego, CA, 92103

Email: wassenaar@degdeg.com

Organization: University of California, San Diego

General Comment

See attached file(s)

Attachments

Koscher Wassenaar

As an academic computer security researcher, BIS's proposed rules for implementing the Wassenaar Arrangement 2013 Plenary Agreements are quite concerning for our field of study, as well as for the computer industry in general. The proposed rules appear to be overly broad and may unintentionally restrict efforts to secure our cyberinfrastructure, as detailed below. At a minimum, BIS should refine its proposed rules and hold a second round of public comments.

1. **The proposed rules may unintentionally cover defensive products.** Whereas traditional software testing focuses on verifying *intended* functionality, software vulnerabilities introduce additional *unintended* functionality. Searching for this additional unintended functionality is difficult because you do not know what you are looking for until you find it. Fortunately, researchers are making progress towards developing tools that *automatically* find such unintended functionalities. These tools can be used by software developers to identify and fix vulnerabilities earlier during the development process. For example, Microsoft has developed and uses a system called SAGE to automatically search for vulnerabilities in its products. However, because these tools discover vulnerabilities, they can also be used offensively. Any new vulnerability found by these tools and not known to the developer would be a "zero-day" exploit. Thus, these types of defensive systems may be subject to controls as software that is used to support development of "zero-day" exploits for sale.
2. **The presumptive denial for "zero-day" exploits is troubling.** Any vulnerability not known to or patched by the manufacturer is a "zero-day" exploit. Does this mean that if I find vulnerabilities in foreign-developed software I am not allowed to share that information with the developer? Due to the vagueness of the rules, people may simply publish the full vulnerability details to the public (i.e., "full disclosure") to avoid any potential export control violations.

In fact, much of our software infrastructure is now developed by teams spread throughout the world. When the OpenSSL vulnerabilities were discovered, there were large, international, coordinated patching and disclosure efforts. If this information cannot be shared before it is made public, then "full disclosure" appears to be the only way forward. Unfortunately, attackers are now able to weaponize fully-disclosed exploits faster than manufacturers can patch. Encouraging "full disclosure," even unintentionally, would be counter-productive to our security.

3. **Deemed exports are problematic for academic research.** In computer science, a large number of graduate students are from outside the US, and since graduate students perform the bulk of federally-funded computer science research, these rules could have a profoundly negative impact on our ability to advance the state-of-the-art in computer security. If these rules go into effect, universities may prohibit international students from working on *anything* related to computer security out of an abundance of caution. Even if universities allow international students to work on some security projects, it may not be possible for international students to work on defensive projects that *could* be used offensively, such as automated vulnerability discovery systems discussed above.

Offensive projects may be even more problematic. For example, we were the first to demonstrate complete remote compromises of modern, unaltered cars. While prior work theorized about the potential problems of “connected cars,” our concrete demonstrations served as a wake-up call to the industry and regulators who are now working diligently to ensure the security of vehicles going forward. As it turns out, one graduate student member of our team was not a U.S. citizen at the time of our work. If our work was impeded by export control concerns, we may have been still oblivious to the true risks of “connected cars.”

These are only a few of the many concerns that I have about the proposed rules, and that I feel that I can provide a unique perspective on. BIS should address these concerns and those from the computer industry and civil liberties advocates, revise the proposed rules, and hold a second round of public comment to ensure that an appropriate balance is reached.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-4ljo
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0180

Comment on FR Doc # 2015-11642

Submitter Information

Name: Travis Roesner

Address:

1855 S Quebec Way

Unit L102

Denver, CO, 80231

Email: travis.roesner@gmail.com

General Comment

I'm but a lowly citizen, but I think that this is one of the worst proposals to come through the United States Government. Encryption is a technology that is already in wide use across the world. If we were to outlaw truly secure encryption in this country, secure encryption would continue to be available in other parts of the world due to open source software repositories not based in the US or other companies that do not care about US laws. (See also: Huawei)

You cannot take freely available software and suddenly decide to take away parts of it in a single country. Especially when most of the internet uses secure encryption to keep United States Citizens secure.

This proposal is akin to trying to put a genie back in a bottle. Secure encryption technology exists, and will continue to exist (and put to use by other regimes aside from the US). Besides, US citizens have a right to privacy, and if secure encryption is compromised it gives not only the FBI / CIA / NSA / etc. access to our private communications, it also gives state-sponsored cyber military units access to them as well.

In short, I will not support any politician or administration that supports this proposal.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-2i9g
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0181

Comment on FR Doc # 2015-11642

Submitter Information

Name: Billy Rios

Address:

1504 Hawser Ln

Half Moon Bay, CA, 94019

Email: billy.rios@whitescope.io

Phone: 4254493830

Organization: Whitescope LLC

General Comment

I've been working in the information security industry for over ten years. I've had the privilege of providing cyber security defense for the Department of Defense, where I helped track hackers who were exploiting Department of Defense information systems. I've also had the privilege of working for both Google and Microsoft within their security engineering departments. While at both Microsoft and Google, I saw firsthand the techniques, tactics, and procedures used by real world hackers to exploit and seek to hurt our users all across the world. Much of our defensive technology and process was built upon things we learned from cutting edge security research. While the proposed changes to the Wassenaar arrangement involving cyber security are likely well intentioned, implementation in its current state will cause tremendous damage to the cyber defensive forces. I am suspicious as to whether the arrangement will be effective in stopping research being done by criminal elements or those wishing to use cyber security to do harm to others. I do however, know that the proposed changes to the Wassenaar arrangement will certainly stifle defensive cyber security research and the sharing of defense cyber security research. As a security engineer who fought to defend Department of Defense computers from hackers and as a security engineer who fought the

rights of dissidents and activists from cyber intrusion, I can honestly say that the proposed changes will put lives at risk.

I realize the development of legislation and policy is difficult. I understand there is currently a need to regulate the proliferation of cyber security technologies being used to exploit and harm people all across the world. While likely well intentioned, the current cyber security proposals to the Wassenaar arrangement are ill-conceived and examine our current cyber security issues through a myopic lens. Let us (the defensive cyber security industry) help you develop the correct approaches to legislation and policy. Together, we can craft the correct legislation and polices to help improve our current situation as it pertains to cyber security.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-5s9n
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0182

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

I'm an IT professional and computer security researcher in Ontario Canada. Though I don't usually comment on American politics, this set of proposed extensions to the INTERNATIONAL Wassenaar Arrangement give me grave cause for concern. The vague, over-arching descriptions of "intrusion software" are so all-encompassing that they could include almost any tool used (in a safe and responsible manner) by myself and members of the international security research community to perform our day-to-day jobs - including the tools required to perform routine security audits of the systems we are paid to protect. It is essentially impossible to distinguish between the tools used by "the bad guys" and "the good guys", so these regulations will inevitably harm the "good guys" trying to do everything legally, legitimately, and above-board, whilst providing no obstacle to the "bad guys" who will of course completely ignore these unenforceable export rules.

The proposed export restrictions resemble a throw-back to the much ridiculed 1990s PGP export controls which made the US a laughing stock in the cryptographic community, indeed leading to a mini "brain drain" and the exclusion of US researchers from most international crypto research.

Please consult properly with internet security professionals before you attempt to regulate something which these amendments appear to woefully misunderstand.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-w3z0
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0183

Comment on FR Doc # 2015-11642

Submitter Information

Name: Nick Galbreath

Address:

Signal Sciences
122 Mildred Ave
Venice, CA, 90291

Email: nickg@signalsciences.com

Phone: 240-779-3980

Organization: Signal Sciences

General Comment

To Whom It May Concern,

Software maps very poorly to traditional notions of "weapons" and "munitions" and it concerns me greatly that the proposed regulations attempts to define them as such. The definitions are vague and the exceptions for research are equally vague. This means anyone working in the software security industry is at the mercy of interpretations of various government jurisdictions. Software and software security is an international endeavor, and these restrictions, real or imagined ,will have a chilling effect on software and defensive security software.

Sadly most software vendors will NOT acknowledge a vulnerability in the software without a fully working exploit (i.e. offensive tooling that makes it easy to exploit). My reading of the proposed exceptions are vague and likely to limit security researchers from going public. In other words, the proposed regulations will likely make security worse.

For me personally, the proposed changes will have a negative impact. As CTO of company working in defensive software technologies, we routinely use these so-called offensive tools regularly. Without them, we can not know what to protect with any certainty. Once the "productized attack" is known, it's fairly easy to provide defensive mechanisms. Without a free-flowing exchange of ideas, our ability to defend is hampered.

While I understand it is appealing going after "offensive" technologies, unfortunately it is misguided and removes focus and responsibility of building secure software in the first place.

Regards,

Nick Galbreath
Chief Technology Officer
Signal Sciences Corporation
Venice, California, USA

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-tefw
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0184

Comment on FR Doc # 2015-11642

Submitter Information

Name: Marsh Ray

Address:

Issaquah, WA, 98029

Email: marshray@live.com

General Comment

I am a US Software Developer and occasional Security Researcher. In the past I have discovered one or more relatively severe flaws in networked protocols and software systems, and I played an active role in these fixes and mitigations working with private companies and through organizations such as the IETF.

While I am deeply sympathetic to the desire to keep tools out of the hands of bad actors, I strongly oppose the proposed regulations as I believe they will actively harm our technical leadership and our data security, while doing little or nothing to achieve the intended goals.

The very nature of our global internet requires that information about vulnerabilities be able to flow freely among those who need it. It commonly happens that the staff who need to urgently become involved in the process are not always able to be predicted in advance. Needed personnel often don't exist within the same organization and are very commonly scattered across several countries. It's generally impossible to ascertain all the business and jurisdictional relationships between an unpredictable-in-advance group of subject matter experts on an urgent basis.

While I support fully open source security research, regulations which attempt to distinguish

between open research and for-pay vulnerability sales are doomed to contain huge gray areas covering entirely non-controversial common cases. Given the incredibly severe penalties for even inadvertently violating an arms control type laws, we can predict that many legitimate researchers will simply avoid any subject matter potentially covered by the agreement, or just publish their results as openly and as quickly as possible giving no advance notification for the affected vendors to prepare mitigations.

Complex and ambiguous regulations such as the proposed are guaranteed to invoke the law of unintended consequences. This will stifle legitimate security researchers and it will delay mitigations. I have seen first-hand the effect of even simple and well-intentioned business agreements complicate matters and cause attempts at coordinated vulnerability disclosure to fall apart.

While it is an unfortunate reality that bad actors are able to benefit from software technologies or leverage little-known flaws, there is probably little or nothing that regulation could do to improve on it. The idea that one could regulate some poorly defined subset of software security tools or vulnerability information as one regulates physical technologies is fundamentally and irreparably flawed.

(These comments and opinions are my own.)

[Duplicate sent via email]

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-aq06
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0185

Comment on FR Doc # 2015-11642

Submitter Information

Name: David Longenecker

Address:

Austin, TX,

Email: dnlongen@gmail.com

Organization: SecurityForRealPeople.com

General Comment

One specific scenario I would like to call out, for which the proposed rules are murky:

Say I explore a network-capable device that I own, for instance a home/small office wireless router, and find exploitable vulnerabilities. If the manufacturer of that device is not a US company, and I submit a bug report to the company in exchange for a "bug bounty" - a payment for finding vulnerabilities - would I run afoul of law?

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-q8tp
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0186

Comment on FR Doc # 2015-11642

Submitter Information

Name: Christopher Soghoian

Address:

PO Box 2266

Washington, DC, 20013

Email: chris@soghoian.net

General Comment

Please see the attached comment, which I submit in my personal capacity.

Attachments

WA Comment - soghoian - final

Christopher Soghoian
PO Box 2266
Washington, D.C. 20013
chris@soghoian.net

Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

July 20, 2015

Re: RIN 0694-AG49, Wassenaar Arrangement Intrusion and Surveillance Items

I thank the Bureau of Industry and Security (“BIS”) for seeking public comment on the proposed Wassenaar Arrangement implementation.

I wish to make it clear that I am filing these comments in my personal capacity.¹

Although I have reservations about the specific draft text that BIS has proposed, I generally support the goal of regulating the export of surveillance technologies. Indeed, I encourage BIS to regulate the export of intrusion and remote monitoring software to governments, such as products similar those sold by FinFisher and Hacking Team,²

I understand that under the current BIS proposal, export controls “would not apply to intrusion software itself (e.g., exploits, rootkits, backdoors, viruses, other malicious code).”³ **I urge BIS to expand the list of controlled technologies, beyond the categories required by Wassenaar.** Specifically, I urge BIS to also regulate the export of security exploits to governments which are explicitly marketed for surveillance purposes, such as products similar to those sold by VUPEN.

I urge BIS to focus its regulations on companies that sell surveillance technologies to governments. BIS should consider both how these surveillance products are marketed, and the end-users to whom they are sold. BIS should adopt a policy of presumptive denial for “lawful interception” products and other surveillance technologies marketed and sold to governments.

¹ My employer, the American Civil Liberties Union (“ACLU”), has not taken a position on BIS' proposed controls of intrusion software. The ACLU has, in the past, publicly opposed export controls governing cryptographic software, and may take a position on this issue at a later date. The opinions expressed in this comment are my own, and do not necessarily reflect the position of the ACLU.

² I understand that Hacking Team, Gamma and VUPEN are all foreign companies. However, they serve as high-profile examples of the types of companies that exist in the surveillance market. Moreover, as described later in this document, US based companies have sold exploits to and facilitated exports for foreign surveillance software companies such as Hacking Team.

³ See http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-06/ispab_june-11_rrarog.pdf at 4.

I also urge BIS to impose “Know Your Customer” obligations on exporters of so-called “lawful surveillance” technologies, similar to those that already exist for nuclear, chemical, and biological weapon end uses.⁴ Given the ease with which products like these can be resold through brokers, export control regulations will only be effective if the manufacturers and exporters of this technology are required to identify the ultimate end-user.

Finally, I urge BIS to make sure that they do not unintentionally chill good-faith computer security research by academics, hobbyists, and the private sector. Whether through unintentionally overbroad language, or simply confusion and misunderstanding by the research community, there is a serious risk that research will be chilled. BIS must make every possible effort to ensure that the final regulations are narrowly crafted, include clear exceptions for good-faith computer security research and are clearly written, such that a non-export control expert can understand them. The US government and economy greatly benefits from good-faith computer security research and so BIS must be careful to make sure that such activities are not chilled.

I. Why Public Pressure Is Not Enough

In 2004, Yahoo! turned over data about two of its users, both Chinese journalists, to the Chinese government. The reporters were subsequently sent to jail, where they alleged they were tortured, for engaging in pro-democracy activities that the Chinese government deemed subversive. Three years later, the U.S. House Foreign Affairs Committee held a hearing to investigate Yahoo! and the assistance that the company provided to Chinese authorities. Addressing Yahoo!’s CEO, who was testifying at the hearing, committee Chairman Tom Lantos stated that: “While technologically and financially you are giants, morally you are pygmies.”⁵

In the wake of that hearing and the negative publicity it generated, Yahoo! settled a lawsuit filed by the imprisoned journalists,⁶ donated one million dollars to Georgetown University to create a fellowship program focused on “international values and Internet and communication technologies,”⁷ and created a Business and Human rights program within the company in order to “define ourselves as an industry leader in this important field.”⁸ Yahoo! also joined with Google and Microsoft to found the Global Network Initiative, in an effort to establish baseline human rights standards for the technology and telecommunications industry.

⁴ See Bureau of Industry and Security, Know Your Customer Guidance, <https://www.bis.doc.gov/index.php/enforcement/oe/compliance/23-compliance-a-training/47-know-your-customer-guidance>.

⁵ See Associated Press, Yahoo Criticized in Case of Jailed Dissident, November 7, 2007, <http://www.nytimes.com/2007/11/07/technology/07yahoo.html>.

⁶ See Associated Press, Yahoo Settles With Chinese Journalists, November 14, 2007, <http://www.nytimes.com/2007/11/14/technology/14yahoo.html>.

⁷ See Yahoo! Fellows Focus On International Values, Georgetown University, <https://giving.georgetown.edu/why-giving-matters/in-action/programs/yahoo>.

⁸ See Michael Samway, Business and human rights, May 7, 2007, <https://yodel.yahoo.com/blogs/yahoo-america/business-human-rights-870.html>.

As U.S Deputy Chief Technology Officer Alexander Macgillivray observed in 2012, while general counsel of Twitter, “No one wants a pen that’s going to rat them out.”⁹ As such, Yahoo! was vulnerable to public pressure because its products were used by the general public, who did not wish to use a surveillance-friendly email service provider, it had a widely recognized public brand that could be easily tarnished, and because increasingly, technology companies are competing on the extent to which they protect their customers’ data from governments.¹⁰

Yahoo! never intended to be in the government surveillance business. While all major technology companies are required to turn over customer data to governments,¹¹ this has until recently, largely been a practice that has been kept out of the public eye, often because companies know it does not look good. Once the human rights impact of Yahoo!’s surveillance assistance was exposed, the company took steps to reform its practices.

In contrast, the companies whose products BIS is seeking to regulate are intentionally in the government surveillance business – often – it is the only business they are in. These firms are not only immune to negative publicity, but in fact bask in it, as the attention can attract new clients.¹² In contrast with Yahoo!, these companies’ brands cannot easily be tarnished, and there is no way for consumers to boycott their products. As such, the only way to control this industry and the global trade in surveillance products is through regulation.

II. The Surveillance Industry

During the past half-decade, the long-shadowy surveillance industry has been forced into the sunlight.¹³ Due to the efforts of journalists, civil society advocates, researchers and an

⁹ See Nick Bilton, A Master of Improv, Writing Twitter’s Script , New York Times, October 6, 2012, <http://www.nytimes.com/2012/10/07/technology/dick-costolo-of-twitter-an-improv-master-writing-its-script.html>.

¹⁰ See Craig Timberg, Apple, Facebook, others defy authorities, increasingly notify users of secret data demands after Snowden revelations, Washington Post, May 1, 2014, http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html.

¹¹ See Christopher Soghoian, The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance, August 2012, Ph.D. dissertation, <http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf> at 17 (“assisting Big Brother has become a routine part of business, albeit one that some service providers would probably rather do without.”)

¹² See Peter Maass, Tweet, July 6, 2015, <https://twitter.com/maass/status/618131011688251392> (“Citizen Lab report outs Hacking Team for privacy invasion, FBI reads report and contacts HT to buy their product.”). See also email from Alex Velasco, Hacking Team Account Manager, July 30, 2014, <https://www.documentcloud.org/documents/2157728-meeting-with-ndcac.html>.

¹³ See Jennifer Valentino-DeVries, Julia Angwin and Steve Stecklow, Document Trove Exposes Surveillance Methods, Wall Street Journal, November 19, 2011. <http://www.wsj.com/articles/SB10001424052970203611404577044192607407780>. See also Sari Horwitz, Shyamantha Asokan and Julie Tate, Trade in surveillance technology raises worries, Wall Street Journal,

unknown, renegade hacker,¹⁴ the public now knows much more about the products these companies sell, and how they are used by their government customers. This increased publicity has led to calls to regulate the industry – which have come from government officials,¹⁵ human rights advocates, and, in some cases, by some in the industry.¹⁶

The companies who create, market and sell these special-purpose spying technologies have not only failed to police themselves, but instead, these ethically bankrupt companies aggressively and unapologetically peddle their wares to despotic regimes, in spite of the well-documented history of human rights abuses by many of their customers. As but one example of this, Tatiana Lucas, the McLean, VA based organizer of the surveillance industry's largest conference, shamelessly described the Arab Spring as a business opportunity for U.S. surveillance companies, and a source of high-tech jobs.¹⁷

There is now ample evidence revealing that authoritarian governments have used surveillance technologies to target political opponents, persecute dissidents, intimidate populations, and to chill free expression. Intrusion software has been used to target Moroccan journalists promoting free speech rights,¹⁸ Bahraini pro-democracy activists,¹⁹ Ethiopian political refugees²⁰ and human rights activists in the United Arab Emirates. In addition to the targeted use of surveillance software against journalists, dissidents and activists, remote monitoring software has also been delivered, indiscriminately, to phones used by innocent people. For example, in 2009, mobile surveillance software was pushed as a “performance update” by Etisalat, the largest wireless carriers in the United Arab Emirates, to more than 100,000 customers with BlackBerry phones.²¹

December 1, 2011, https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html.

¹⁴ See Lorenzo Franceschi-Bicchierai, Hacker Claims Responsibility for the Hit on Hacking Team, Motherboard, July 6, 2015,

<http://motherboard.vice.com/read/hacker-claims-responsibility-for-the-hit-on-hacking-team>

¹⁵ See Jennifer Baker, Stop selling spyware to despotic regimes, beg MEPs, The Register, 27 November, 2014,

http://www.theregister.co.uk/2014/11/27/stop_selling_spyware_to_despotic_regimes_beg_meps_weve_enough_trouble_here/.

¹⁶ See Email from Adriel T. Desautels to Daily Dave email list, August 14, 2012,

<http://marc.info/?l=dailydave&m=134506034828926> (“Oh I think [the zero day trade] has the potential to cause harm, especially in the wrong hands... which is why I think that the zero-day exploit market should be regulated. We're selling bullets and computers are the guns, there's no doubting that.”)

¹⁷ See Tatiana Lucas, Web Surveillance Software and Jobs, The Wall Street Journal, December 9, 2011, <http://www.wsj.com/articles/SB10001424052970204770404577082623956166242>.

¹⁸ See Ryan Gallagher, How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists, Slate, August 20, 2012,

http://www.slate.com/blogs/future_tense/2012/08/20/moroccan_website_mamfakinch_targeted_by_government_grade_spyware_from_hacking_team_.html.

¹⁹ See Morgan Marquis-Boire, Bill Marczak, From Bahrain With Love: FinFisher's Spy Kit Exposed?, Citizen Lab, July 25, 2012, <https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/>.

²⁰ See Privacy International, Criminal complaint to National Cyber Crime Unit on behalf of Tadesse Kersmo, <https://www.privacyinternational.org/?q=node/80>.

²¹ See George Bevir, Etisalat's BlackBerry patch designed for surveillance, July 14, 2009, ITP.net, <http://www.itp.net/561962-etisalats-blackberry-patch-designed-for-surveillance>.

The technologies used in these cases were not locally sourced, but rather, were provided by Western-based companies, many with offices in the United States. The mobile surveillance software pushed by Etisalat to its customers was made by SS8, a “lawful surveillance” technology company based in Milpitas, California. Similarly, Hacking Team, an Italian provider of remote monitoring software, sold its products to Sudan, Azerbaijan, Uzbekistan, Ethiopia and a number of other countries with well-documented histories of abusing human rights.²²

In some cases, these same companies provide on-site installation and training,²³ as well as ongoing software updates, tech-support and custom, hand-crafted surveillance solutions. For example, Area SpA, an Italian surveillance company, sent engineers to Syria to install an IP surveillance system capable of intercepting, scanning and cataloging virtually every email transmitted in the country for Bashar al-Assad’s regime.²⁴ Similarly, if governments are not able to compromise a target using the exploits and malware provided to them by Hacking Team, the company also offers a consultancy service capable of creating bespoke solutions for “complicated [surveillance] scenarios.”²⁵

III. The Need For Regulation

Despite the well-documented misuse of surveillance technology, including intrusion software and IP surveillance systems, by authoritarian governments,²⁶ the surveillance industry has failed to regulate itself. The manufacturers of this technology have made it clear that they do not believe that they have a responsibility to evaluate their potential clients, and, when pushed, claim that governments are better suited to the task of approving or prohibiting surveillance technology sales.

Like Wernher Von Braun,²⁷ many in the surveillance industry argue that they are not responsible for how their products are used.²⁸ Not only have many of these companies

²² See Alex Hern, Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim, *The Guardian*, July 6, 2015, <http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim>.

²³ See Utimaco LIMS Lawful Interception of Telecommunication Services Brochure page 8, https://www.documentcloud.org/documents/804662-1241_utimaco_product-description.html#document/p8/a129476%2066.

²⁴ See Vernon Silver, Syria Crackdown Gets Italy Firm’s Aid With U.S.-Europe Spy Gear, *Bloomberg*, November 3, 2011, <http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear>.

²⁵ See <https://ht.transparencytoolkit.org/rcs-dev%5cshare/Documentation/Presentations/RCS%20%20Attack%20Vectors.pptx> at page 15-16.

²⁶ See Ryan Gallagher, French Company That Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations, *Slate*, June 19, 2012, http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi_.html; See also Privacy International, Privacy International files criminal complaint on behalf of Bahraini activists targeted by spyware FinFisher, October 13, 2014, <https://www.privacyinternational.org/?q=node/451>.

²⁷ See Tom Lehrer, in lyrics to "Wernher von Braun", <https://www.youtube.com/watch?v=TjDEsGZLbio>, (“Once the rockets are up who cares where they come down that's not my department”)

²⁸ See Ben Nagy, email to Daily Dave mailing list, April 5, 2012, <https://lists.immunityinc.com/pipermail/dailydave/2012-April/000088.html> (“I spend my time milling

compared their products to neutral household items that might possibly be abused,²⁹ but some explicitly reject any ethical obligation to evaluate how their clients will use their products. For example, Donato Ferrante, a seller of zero-day security exploits stated that “I don't see bad guys or good guys... It's just business.... The way the information is used is up to the customer; it's not up to us.”³⁰ Hacking Team's Eric Rabe has stated that “I don't think we're in the business of policing” how the firms' surveillance software is used.³¹ Similarly, Adriel Desautels of Massachusetts-based Netragard has stated that “[w]hat our customers do with the exploits that they buy is none of our business just as what you do with your laptop is not its vendors business.”³²

Both Hacking Team and Gamma (now FinFisher) have publicly stated that they have internal processes in place to evaluate potential clients. It appears that these internal ethics and human rights assessments serve as mere window dressing. In some cases, these efforts border on the absurd. Gamma, for example, apparently appointed a “human rights officer” to its board of directors to help the company evaluate the human rights risks associated with new clients. That position was filled by Martin Münch, the Managing Director of the company,³³ who Bloomberg had described in a profile as “personified evil.”³⁴

cyber-gunpowder for people that make cyber-bullets sold by ‘modern-day cyber-merchants of death’. I am the frumpish british mother that filled the shells for the fire-bombing of Dresden. I am the Wal-Mart attendant that sold the gun to the father of the last school shooter. I do it for money, because I like it, and because most of the time I don't need to wear pants. I spend approximately no seconds of any day worrying about the imaginary ethical implications of every little thing I do, and I am not particularly unique.”)

²⁹ Jerry Lucas, the organizer of the ISS World surveillance industry conference has compared surveillance technology to cars, “You can sell cars to Libyan rebels, and those cars and trucks are used as weapons. So should General Motors and Nissan wonder, ‘how is this truck going to be used?’ Why don't you go after the auto makers?” See Ryan Gallagher, Governments turn to hacking techniques for surveillance of citizens, *The Guardian*, November 1, 2011, <http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance>. Gamma's Münch also argues that his products can be both used legitimately and illegitimately, comparing them to “a can of fizzy drink or a car battery” which can be misused in the wrong hands. See Vernon Silver, MJM as Personified Evil Says Spyware Saves Lives Not Kills Them, *Bloomberg*, November 8, 2012, <http://www.bloomberg.com/news/articles/2012-11-08/mjm-as-personified-evil-says-spyware-saves-lives-not-kills-them>.

³⁰ See Tom Gjelten, In Cyberwar, Software Flaws Are A Hot Commodity, *NPR*, February 12, 2013, <http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity>.

³¹ See Reply All (podcast), *The Evilest Technology On Earth :-)*, July 15, 2015, at 11:55, <https://gimletmedia.com/episode/32-the-evilest-technology-on-earth/>.

³² See Adriel Desautels, Netragard on Exploit Brokering, <https://www.netragard.com/netragard-on-exploit-brokering>.

³³ See Jasmin Klofta, Frederick Obermeier, Bastian Brinckmann, Selling spyware to trap dissidents, *Süddeutsche Zeitung*, February 22, 2013, <http://www.voxeurop.eu/en/content/article/3449501-selling-spyware-trap-dissidents> (“Nevertheless, Münch is now promising a change: more transparency, real consequences. Gamma is going to put a human rights officer on its board of directors soon. He'll probably be assigned the title himself, adds Münch. Rather an odd choice, though: after several hours' interviewing Martin Münch, one still has the impression that there's no needle on his moral compass.”)

³⁴ See Vernon Silver, MJM as Personified Evil Says Spyware Saves Lives Not Kills Them, *Bloomberg*, November 8, 2012, <http://www.bloomberg.com/news/articles/2012-11-08/mjm-as-personified-evil-says-spyware-saves-lives-not-kills-them>.

Similarly, Hacking Team's CEO publicly stated that his firm follows "strict ethical guidelines,"³⁵ and that "[w]e pay the utmost attention to whom we are selling the product to." He stated that his company had set up "a legal committee", which was quietly disbanded in 2015,³⁶ "whose goal is to promptly and continuously advise us on the status of each country we are talking to. The committee takes into account UN resolutions, international treaties, Human Rights Watch and Amnesty International recommendations."³⁷ After the company was hacked in June of 2015, media reports revealed that the company had in fact obtained a biannual review of its clients by an outside law firm, but that this had not prevented the company from selling its software to a large number of countries with well-documented records of abusing human rights.³⁸

Some of the most high-profile suppliers of remote monitoring software and security exploits have stated that they do not see it as their role to evaluate their customers, and suggest that this is a role better left to governments and export control authorities. Both VUPEN and Hacking Team have publicly pledged that they will not sell products to countries that have been placed on international blacklists.³⁹ VUPEN's CEO has suggested that if human rights advocates have a problem with the company selling exploits to a particular government, they should "write to [the] European Union and the US to add them to the [black]list."⁴⁰ Jerry Lucas of ISS World has stated that "[It's] just not my job to determine who's a bad country and who's a good country. That's not our business, *we're not politicians* ... we're a for-profit company."⁴¹ Gamma's Münch has been even more direct, stating that "rather than pay lip service to 'ethics', *we have decided to let the export controls authorities act as our 'moral compass'*, for want of a better expression. After all, they are best placed to know who the 'bad guys' are and who the likely future 'bad guys' will be. We follow their lead and comply with the law."⁴²

IV. The Role of American Intermediaries

Although many of the most high-profile players in the remote monitoring software industry are European, the recent compromise of Hacking Team's emails and other

³⁵ See Angus Batey, The spies behind your screen, The Telegraph, November 24, 2011, <http://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html>.

³⁶ See Collin Anderson, Tweet, July 6, 2015, <https://twitter.com/CDA/status/618222979894366212>.

³⁷ See Ryan Gallagher, Hacking Team: Mass Surveillance Made In Milan, August 27, 2012, <http://notes.rjgallagher.co.uk/2012/08/hacking-team-milan-surveillance-rcs-interception.html>.

³⁸ See Cora Currier and Morgan Marquis-Boire, A Detailed Look At Hacking Team's Emails About Its Repressive Clients, The Intercept, July 7, 2015, <https://firstlook.org/theintercept/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/>.

³⁹ See Hacking Team, Customer Policy, <http://www.hackingteam.it/index.php/customer-policy> ("We do not sell products to governments or to countries blacklisted by the U.S., E.U., U.N., NATO or ASEAN.")

⁴⁰ See Chaouki Bekrar, Tweet, September 11, 2012, <https://twitter.com/cbekrar/status/245525072855580674> ("We don't even know where that country is, anyway if you are not happy write to European Union and the US to add them to the list").

⁴¹ See Ryan Gallagher, Governments turn to hacking techniques for surveillance of citizens, The Guardian, November 1, 2011, <http://www.guardian.co.uk/technology/2011/nov/01/governments-hacking-techniques-surveillance>.

⁴² See Ryan Gallagher, Spy Trojan Seller on Ethics, Authoritarians, & 'Bad Guys' vs. 'Good Guys' March 11, 2013, <http://notes.rjgallagher.co.uk/2013/03/gamma-finspy-surveillance-ethics-martin-muench.html>.

documents has shed light on the extent to which US-based firms have supplied the company with security exploits and facilitated exports to authoritarian governments.

Adriel Desautels, the president of Netragard, an exploit broker based in Massachusetts, told Slate in 2013 his company had adopted a policy to sell his exploits only domestically within the United States. He also told the reporter that he rigorously vetted the companies who to whom he sold exploits.⁴³ In an email to Hacking Team's Chief Operating Officer in March of 2015, Desautels stated that "We've been quietly changing our internal customer policies and have been working more with international buyers... We do understand who your customers are both afar and in the US and are comfortable working with you directly."⁴⁴

Hacking Team's emails confirmed both that Netragard had sold a software exploit to Hacking Team (via a US-based affiliate), and that this sale had taken place after researchers and the media had revealed that Hacking Team had provided surveillance software to authoritarian governments which had used the software to target reporters and political dissidents. When interviewed by one reporter, Desautels revealed that "I heard news about Hacking Team being questionable and so on, but it was the same kind of fodder, or [Fear, Uncertainty and Doubt], that we hear all the time about zero-days."⁴⁵ In short, although Desautels was aware of reports that Hacking Team's software was being misused by its government clients, he did not read the reports and went along with the sale. Desautels continues to insist that he bears no responsibility for how Hacking Team's clients may have used the exploit he sold to the company.⁴⁶

In addition to the role of US exploit brokers, the publication of Hacking Team's emails also reveals the role of US-based resellers and intermediaries. Internal company documents show Azerbaijan's Ministry of Defense purchased a license for Hacking Team's surveillance software via a California-based intermediary called Horizon Global Group in 2013.⁴⁷ Horizon Global Group has no online presence, public profile, or listed phone number and lists its address as a PO Box in "Ranchos Palos Verdes, Nevada, CA 90274."

⁴³ See Ryan Gallagher, *Cyberwar's Gray Market*, Slate, January 16, 2013, http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gra_y_market_be_regulated.html.

⁴⁴ See email from Adriel Desautels to Giancarlo Russo, March 6, 2015, <https://wikileaks.org/hackingteam/emails/emailid/15116>.

⁴⁵ See Joseph Cox, *Where Did Hacking Team Buy Its Hacks? Three Accused Brokers Deny Wrongdoing*, Motherboard, July 13, 2015, <http://motherboard.vice.com/read/where-did-hacking-team-buy-its-hacks-three-accused-brokers-deny-involvement>.

⁴⁶ See Adriel Desautels, *Tweet to Christopher Soghoian*, July 9, 2015, <https://twitter.com/greybrimstone/status/619336476296409088> ("so wait, you think that we are responsible for HT's decision to resell to questionable buyers? Are you an idiot?").

⁴⁷ See Organized Crime And Corruption Reporting Project, *Azerbaijan bought Hacking Team's surveillance spyware, leaks reveal*, July 8, 2015, <https://www.occrp.org/en/daily/4136-azerbaijan-bought-hacking-team-s-surveillance-spyware-leaks-reveal>. See also https://ht.transparencytoolkit.org/Amministrazione/01%20-%20CLIENTI/2%20-%20Fatture/4%20-%20Fatture%202013/5%20-%20Maggio/Fattura%20-%20025_2013%20-%20Horizon%20Global%20Group.pdf.

V. Recommendations

A. Exploits

There exists significant confusion about whether or not BIS intends for zero-day vulnerabilities and exploits to be regulated. The proposed implementation states that “proprietary research on the vulnerabilities and exploitation of computers and network-capable devices” is regulated. However, in an online FAQ published afterwards, BIS suggested that exploits and “the code that takes advantage of the vulnerability would not require a license.”⁴⁸ Although BIS states that the proposed rules do not control “Information about the vulnerability, including causes of the vulnerability”, BIS’s distinction between this and information for developing the exploit, which is regulated, is not clear.

I urge to provide much-needed clarity to this question, and to go further by clearly and unambiguously regulating the export of software exploits to governments which are explicitly marketed for surveillance purposes. Companies such as VUPEN, Hacking Team and Austin, TX-based Exodus Intelligence clearly advertise surveillance uses of their products,⁴⁹ while VUPEN and Hacking Team only sell their products to governments.

Narrowly drafted regulations that control the export of exploits to governments that are advertised for surveillance uses will of course not address problematic exports of exploits by companies that either do not advertise specific uses or that sell to non-governmental clients (who then subsequently re-sell those exploits to governments). Given that some of the worst offenders in the surveillance industry, whose products have been sold to human-rights abusing governments, currently advertise their products as intended for surveillance uses, exhibit them at surveillance conferences, and sell directly to governments, I believe that narrow, strict regulation of such exports will be a good first step, and will minimize the risk of unintentional harm to the computer security community. If, in response to such regulations, the surveillance industry merely changes the way they market their products, BIS can re-visit the issue.

⁴⁸ See Bureau of Industry and Security FAQ, Intrusion and Surveillance Items, <https://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>, (Last visited June 9, 2015).

⁴⁹ See <https://www.exodusintel.com/capabilities.html> (“The United States FBI has utilized zero-day exploits to assist in their Lawful Intercept efforts, specifically to deploy their Computer and Internet Protocol Address Verifier (CIPAV) software on target criminal's computers....The FBI has been using the CIPAV since 2002 against hackers, online sexual predators, extortionists, and others, primarily to identify suspects who are disguising their location using proxy servers or anonymity services, like Tor.”)(describing the use of exploits by law enforcement as a “specialized use case” for its products).

See also <https://ht.transparencytoolkit.org/rcs-dev%5cshare/Documentation/Presentations/RCS%208%20Attack%20Vectors.pptx> (describing the use of security exploits, provided by the company, as “attack vectors” to gain access to a target’s system in order to then deliver the RCS surveillance software.”)

B. Take Into Account The End-Users Of Surveillance Products And The Way That They Are Marketed

The difficulties of regulating intrusion software and IP surveillance systems can be greatly mitigated by considering both the end-users of the products and the ways in which they are advertised.

The unregulated nature of the surveillance industry, which is estimated to be worth five billion dollars per year,⁵⁰ lends itself towards competition among suppliers. Surveillance companies advertise their products at tradeshows attended by government customers, many with abysmal human rights records, to highlight differentiating capabilities and features.⁵¹ These firms are not shy about advertising their products' capabilities and intended uses, often through detailed marketing materials.⁵²

I believe that BIS can and should draw a distinction between general-purpose cybersecurity technologies, which can be used in good and bad ways by private parties, corporations and governments, and surveillance technologies explicitly marketed to and only sold to governments. I urge BIS to adopt a policy of presumptive denial for "lawful interception" products and other surveillance technologies marketed to governments. This would include, for example, many, if not most of the products sold by companies that exhibit at conferences like ISS World.

C. Extend "Know Your Customer" Requirements To Exploit And Vulnerability Exports

Several major surveillance companies, including VUPEN and Hacking Team claim they have adopted "Know Your Customer" ("KYC") processes intended to limit the abuse of their products.⁵³ This process is, it seems, slowly becoming an industry best practice. I

⁵⁰ See Sari Horwitz, Shyamantha Asokan and Julie Tate, Trade in surveillance technology raises worries, Wall Street Journal, December 1, 2011, https://www.washingtonpost.com/world/national-security/trade-in-surveillance-technology-raises-worries/2011/11/22/gIQAFFZOGO_story.html.

⁵¹ See Lisa Evans, Surveillance trade shows: which government agencies attend?, The Guardian, February 7, 2012, <http://www.theguardian.com/news/datablog/2012/feb/07/surveillance-shows-attendees-iss-world> (Listing surveillance trade show attendees: Bahrain, Turkey, Sudan, Somalia, Russia, Qatar, China, Egypt and Democratic Republic of the Congo, among many others).

⁵² See generally, <https://wikileaks.org/the-spyfiles.html>.

⁵³ See <https://web.archive.org/web/20150204102921/http://www.vupen.com/english/services/lea-index.php> ("All subscription requests are subject to a case-by-case and thorough analysis. Even if an organization fully meets all applicable regulations and complies with our 'Know Your Customer' program,") (linking to the BIS know your customer regulations). See also <http://www.hackingteam.it/index.php/customer-policy> ("HT policies and procedures are consistent with the U.S. Know Your Customer guidelines. We conduct ongoing employee training to assure that employees know and understand the provisions of these guidelines. Should we discover "red flags" described in these guidelines while negotiating a sale, we will conduct a detailed inquiry into the matter and raise the issue with the potential customer. Our review will include:

- Statements made by the potential customer either to HT or elsewhere that reflect the potential for abuse;
- The potential customer's laws, regulations and practices regarding surveillance including due process requirements;

recommend that BIS mandates that all companies exporting surveillance technology be capable of demonstrating that they, at a minimum, have satisfied the KYC process before, during and after a sale.⁵⁴

Although BIS has imposed KYC requirements for nuclear, chemical, and biological weapon end uses,⁵⁵ no such obligation exists for surveillance technology. End-uses of surveillance technology that result, or are likely to result in human rights violations warrant KYC protection, and should be implemented for Intrusion Software, IP Surveillance Systems, and security exploits. Standard red flags should also be promoted that mitigate transshipment risks and identify changes in customer needs, network placement, and communication with update servers.⁵⁶

If the KYC process reveals objective evidence or credible concerns that the sale of the vulnerability or exploit will be used to facilitate human rights violations, the individual or company should be obligated by BIS to refrain from participating in the transaction.

Moreover, selling to a vulnerability broker without considering the end use must be considered by BIS as a form of self-blinding, or restricting one's own knowledge of the end-use through a lack of requested or sought out information. Similarly, brokers like Netragard, who keep the identities of the buyer and seller from each other,⁵⁷ should also be considered to be facilitating self-blinding. As recognized by BIS, “[a]n affirmative policy of steps to avoid ‘bad’ information would not insulate a company from liability, and it would usually be considered an aggravating factor in an enforcement proceeding.” Every effort must be made by individuals and companies to identify the end-use of the exploit or vulnerability.

The minimum required steps for the “Know Your Customer” process, adapted from the Electronic Frontier Foundation’s guidance, are as follows:

1. Review the capabilities of the exploit or vulnerability for human rights abuses and consider possible mitigation measures, both technical and contractual.

-
- Credible government or non-government reports reflecting that a potential customer could use surveillance technologies to facilitate human rights abuses.”

⁵⁴ These recommendations draw heavily on the process outlined by the Electronic Frontier Foundation. See Electronic Frontier Foundation, “Know Your Customer” Standards for Sales of Surveillance Equipment, Oct. 24th, 2011, <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>.

⁵⁵ See Bureau of Industry and Security, Know Your Customer Guidance, <https://www.bis.doc.gov/index.php/enforcement/oe/compliance/23-compliance-a-training/47-know-your-customer-guidance>.

⁵⁶ See Collin Anderson, Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies, Access, March 9, 2015, https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf.

⁵⁷ See Adriel Desautels, Tweet, July 15, 2015, <https://twitter.com/greybrimstone/status/621374601633886208> (“Something to note, we don’t develop 0-day’s in house, we only broker them. We keep the parties involved anonymous.”)

2. Review what the purchasing individual, government, or company is saying about the use of exploits or vulnerabilities, both before and during any transaction. This includes, among other things, review of sales and marketing materials and discussions, technical discussions and questions, presentations, technical and contractual specifications and technical support conversations or requests.
3. Review the laws of the country in which the vulnerability or exploit will be operated, regulations and practices regarding surveillance, including interception of communications, access to stored communications, due process requirements, and other relevant legal process as part of the assessment of risk of how the vulnerability or exploit may be used.
4. Review U.S. State Department annual human rights reports, relevant U.N. Reports, and other credible reports about the government, company or individual, including news or other reports from nongovernmental sources or local sources that indicate whether they use surveillance technology in such a way that results in human rights abuses.

D. Protecting Good-Faith Research

Currently, Title 15 of the Code of Federal Regulations, Section 734.8⁵⁸ exempts information arising during, or resulting from fundamental research from the Export Administration Regulation.⁵⁹ Source code and other software are, of course, forms of information.⁶⁰ Fundamental research is said to be performed in industry, Federal laboratories, or other types of institutions, as well as in universities.⁶¹ The Code notes, however “it remains the type of research, and particularly the intent and freedom to publish, that identifies ‘fundamental research,’ not the institutional locus.”⁶² On a plain reading of the above provisions, it appears that the research conducted by security researchers using cybersecurity items working independently and outside any

⁵⁸ See Export Administration Regulations, Section 734 (November 2014), https://www.bis.doc.gov/index.php/forms-documents/doc_view/412-part-734-scope-of-the-export-administration-regulations_

⁵⁹ *Id.* §734.3 (b)(3)(ii).

⁶⁰ See Electronic Privacy Information Centre, American Civil Liberties Union, et. al., BRIEF FOR AMICI CURIAE, Daniel J. Bernstein v. United States Department of Commerce, et. al. (November 1997), https://epic.org/crypto/export_controls/bernstein_brief.html (The Export Administration Act divides the subjects of its export control regime into two mutually exclusive categories: "goods" and "technology." The Act defines "goods" as "any article, natural or manmade substance, material supply or manufactured product, . . . *excluding technical data.*" 50 U.S.C. App. ' 2415(3) (emphasis added). "Technology" is defined in turn to encompass "*information or know-how* [tangible or intangible] that can be used to design, produce, manufacture, utilize or reconstruct goods, *including computer software* and technical data, but not the goods themselves." 50 U.S.C. App. § 2415(4) (emphasis added). The Regulations, based on the Act, follow an exactly parallel structure and thus distinguish between mutually exclusive categories of "commodities" and "technology." Indeed, the Regulations expressly define "commodities" to include "[a]ny article, material, or supply *except technology and software.*" 15 C.F.R. pt. 772 (emphasis added). Reflecting that division, software has always been treated under the EAR as a form of technology -- *i.e.*, information or know-how -- and not as a commodity.).

⁶¹ *Id.* Supplement No. 1 to part 734 page 4.

⁶² *Id.*

institutional context towards public publication may not be readily considered fundamental research.

The information security research community is made up of geographically distributed independent researchers that make invaluable contributions to global cybersecurity. Many work in their spare time, do not hold advanced academic degrees and do not receive any funding for their research. BIS should specify that no institutional affiliations are required have research classified as fundamental. As long as the researcher engages in good-faith basic and applied research in science or engineering, “where the resulting information is ordinarily published and shared broadly within the scientific community,”⁶³ the research and tools used should be exempted.

In addition to exempting private coordination towards publicly released cybersecurity item research, BIS should exempt vulnerability research and enabling tools if it is conducted with the intention of disclosing the vulnerability to the software vendor, regardless of whether the results of the research are made public. Any research which results in the private disclosure to the vendor responsible for the software should be exempted as well.

E. Protecting Bug Bounties

For far too long, researchers who discovered a security vulnerability have had to make a difficult choice: do the right thing—by telling the company responsible for the software or warning the general public—or sell the vulnerability, often to a government, which would then quietly exploit that flaw for its own gain.⁶⁴

In an effort to disrupt this shadowy grey market and to provide some financial reward to researchers who notify the responsible vendor or developers, some leading technology companies have created “bug bounty” programs. These programs, which have been adopted by Google,⁶⁵ Microsoft,⁶⁶ Facebook,⁶⁷ Yahoo,⁶⁸ Twitter,⁶⁹ Snapchat,⁷⁰ and others offer researchers thousands (and, in some cases, tens of thousands) of dollars per vulnerability. Some software vendors also offer rewards for discovering vulnerabilities in software made by other companies and organizations.⁷¹

In addition to bug bounties, there also exists bug challenges and auctions, which offer varying monetary rewards for the discovery of software vulnerabilities, and vulnerability

⁶³ See 15 CFR 734.8.

⁶⁴ See Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*, Independent Security Evaluators, May 6, 2007, <http://weis2007.econinfosec.org/papers/29.pdf>.

⁶⁵ See Google Vulnerability Reward Program (VRP) Rules, Google <http://www.google.com/about/appsecurity/reward-program/> and Chrome Reward Program Rules, Google, <http://www.google.com/about/appsecurity/chrome-rewards/>.

⁶⁶ See Microsoft Bounty Programs, Microsoft, <https://technet.microsoft.com/en-us/library/dn425036.aspx>.

⁶⁷ See Whitehat, Facebook, <https://www.facebook.com/whitehat>.

⁶⁸ See Yahoo!, Hacker One, <https://hackerone.com/yahoo>.

⁶⁹ See Twitter, Hacker One, <https://hackerone.com/twitter>.

⁷⁰ See SnapChat, Hacker One, <https://hackerone.com/snapchat>.

⁷¹ See Google Patch Reward Program, Google, <https://www.google.com/about/appsecurity/patch-rewards/>.

brokers, who acquire vulnerabilities from researchers and distribute information about them to customers or subscribers.⁷² Organizations like the Zero Day Initiative (“ZDI”) encourage researchers to responsibly disclose vulnerabilities through a transparent and legal process, rather than sell them to vulnerability brokers on the black or grey market.

Participation in bug bounties, challenges and auctions, or any program that is intended to result in the timely disclosure of the vulnerability to the public or the impacted software vendor should be exempted. These programs genuinely improve global cybersecurity and provide deserved remuneration to researchers. BIS must not shift incentives away from these programs towards the ethically dubious grey market.

F. The Regulations And All Exceptions Must Be Clearly Understandable By Non-Lawyers

The computer security community operates under what can reasonably be described as hostile legal conditions. Researchers engaging in socially beneficial research regularly face legal threats and risks of litigation under both the Digital Millennium Copyright Act⁷³ and the Computer Fraud and Abuse Act.⁷⁴ Similarly, after fighting, and winning the first “crypto-war” in the 1990s, the community now faces the prospect of potential legislation requiring the insertion of surveillance backdoors in encryption technology.

As such, no matter how pure BIS’ intentions are, or how obvious the existing exceptions are to the lawyers who have drafted them, the proposed regulations have already been met with suspicion and fear of overreach. Research has already been chilled, largely because many researchers simply do not understand whether or not their own research is currently controlled.⁷⁵ Computer security researchers are not export control lawyers, and naturally assume the worst.

Going forward, I urge BIS to make sure that all regulations and exemptions that might potentially impact the computer security computer be unambiguously written so that they can be understood by non-export control experts. The computer security community should know what rules, if any, apply to them, and not be unnecessarily chilled due to lack of clarity in the rules.

⁷² See Rainer Böhme, A comparison of market approaches to software vulnerability disclosure. In *Emerging Trends in Information and Communication Security* (pp. 298-311). Springer Berlin Heidelberg, March 2006, http://www.is.uni-muenster.de/security/publications/boehme2006_compvulnmarkets_etrics.pdf.

⁷³ See Electronic Frontier Foundation, *Unintended Consequences: Fifteen Years under the DMCA* (March 2013), <https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca>.

⁷⁴ See Electronic Frontier Foundation, *Computer Fraud and Abuse Act Reform*, <https://www.eff.org/issues/cfaa>.

⁷⁵ See Alexander J Martin, *Export control laws force student to censor infosec research*, *The Register*, July 3, 2015, http://www.theregister.co.uk/2015/07/03/northumbria_university_ethical_hacking_student_forced_censor_disseration.

VI. Conclusion

BIS has taken on an extremely difficult task, for which it has received significant criticism, much of it justified, from the computer security community. I hope that BIS will carefully consider my comments and those submitted by other organizations, companies and individuals, revise the proposed regulations, and then seek an additional round of public comments.

Thank you.

Christopher Soghoian, Ph.D.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-5ywu
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0187

Comment on FR Doc # 2015-11642

Submitter Information

Name: Steve Roggenkamp

General Comment

It seems to me this is a well intensioned, but flawed attempt to control the export of intrusion software.

According to question 28 in Intrusion and Surveillance Items, 'Does "publicly available" as understood by the BIS include posting to the internet?' could be interpreted to include posting to the Dark Web where one can find many things normally considered illegal if one has the persistence to find them. It seems to me this could provide a huge loophole to getting around the provisions of this proposal, thus rendering it ineffective.

Providing a Marketing exclusion in section 5A001.j also provides a huge loophole for this proposal.

There is little difference between what a marketer and a malware author are attempting to do. In most cases both of them are attempting to get a user to click on a link in order to acquire a resource from a user whether it is money in exchange for a good or service in the case of a "legitimate" marketer, or data or something else in the case of malware. In many cases there is very little difference between the two classes of interaction. Allegedly legitimate marketers have installed so-called adware which consume resources and may communicate to their command and control systems. There is very little distance between software such as this, which would be sanctioned by these rules, and the criminal systems which install software on computers for nefarious purposes such as spying or extortion.

I also see this as having a chilling effect on international collaboration in terms of cybersecurity research, especially in the early stages of an exploit project.

Questions 2 through 5 in Intrusion and Surveillance Items seem to indicate that a researcher publishing information about an exploit would be exempt from the provisions of the agreement. However, it is unclear to me whether international collaborators would be covered during their research phase leading up to publication of their findings. I can think of many scenarios where communications between researchers could run afoul of this agreement.

For these reasons I believe this is a bad agreement that will do little to increase the security of my systems over time.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-hc76
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0188

Comment on FR Doc # 2015-11642

Submitter Information

Name: Sergey Bratus

Address:

6211 Sudikoff

Hanover, NH, 03755

Email: sergey@cs.dartmouth.edu

Phone: 603 646 9224

General Comment

Please find attached my comments on BIS-2015-0011.

Attachments

bis-public-comment-with-faq-notes

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-kbqb
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0189

Comment on FR Doc # 2015-11642

Submitter Information

Name: Berin Szoka

Address:

110 Maryland Ave NE, Suite 407

Washington, DC, 20002

Email: media@techfreedom.org

Phone: (917) 744-0387

Organization: TechFreedom

General Comment

See attached file(s)

Attachments

TechFreedom Comments on BIS Wassenaar Rule for Cybersecurity

TECH FREEDOM

Comments of

TechFreedom

Berin Szoka, President

Mark Potkewitz, Summer Fellow

In the Matter of

Department of Commerce, Bureau of Industry and Security

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items
(Proposed Rule with request for comments)

Docket No. 150304218–5218–01

July 20th, 2015

The Bureau of Industry and Security's (BIS) "Proposed Rule" seeks comments on the implementation of the Wassenaar Arrangement which would add a license requirement to selected "cybersecurity items."¹ The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies ("Wassenaar Arrangement"), a multilateral export control regime, aims to increase international and regional stability by restricting exports of certain munitions and goods along nine main categories with two annexes delineating *sensitive* and *very sensitive* items.

In principle, we support BIS's effort to minimize the export of U.S. technologies to regimes that will use them against their own citizens. Yet we also recognize that these technologies are necessary for those citizens to defend themselves — and that controlling the transfer of cybersecurity technologies will necessarily burden defense as well as offense, circumvention as well as censorship.

Thus, we were heartened that the Proposed Rule includes the following refreshingly candid admission:

The impact of this rule is unknown to BIS, therefore the implementation of the Wassenaar Arrangement agreement of 2013 with regard to cybersecurity items is issued as a proposed rule with request for comments concerning the impact of the rule.

If only more regulators were so willing to admit "how little they really know about what they imagine they can design" — to use the most famous line from *The Fatal Conceit*, F.A. Hayek's 1988 magnum opus about the perils of top-down planning.² Illustrating this, as Hayek argued, is "the curious task of economics": to probe the likely consequences, as far as can be foreseen, of any possible regulation. It is also what BIS must do if it is to balance liberty with security in the broadest sense.

In this case, the costs and benefits of restraining the flow of cybersecurity technologies are both economic, in the traditional sense of financial costs for companies and effects on markets, and "non-economic," in the broader sense of costs that are more difficult to quantify in financial terms. Among the trade-offs that must be considered are:

- Will U.S.-based cybersecurity firms move overseas?
- Will foreign-based cybersecurity firms be reluctant to do business with U.S. customers and firms?
- Will new rules make it more difficult for foreign system operators, both private and public, and individuals to defend themselves from attack?
- Will new rules undermine cybersecurity research?
- Will new rules hamper collaborative efforts between international security experts?
- Will new rules prevent firms with international offices from using the same tools across offices?
- How will new rules affect cybersecurity startups, in particular?

¹ Department of Commerce Bureau of Industry and Security, 80 Fed. Reg. 97 (May 20, 2015), available at http://www.bis.doc.gov/index.php/forms-documents/doc_download/1236-80-fr-28853 .

² Friedrich Hayek, *The Fatal Conceit: The Errors of Socialism* 76 (1988).

Whether BIS is legally *required* to engage in any form of cost-benefit analysis is irrelevant to whether it *should* do so. Indeed, Executive Order 13563 — which the Proposed Rule specifically cites, without any further commentary — makes no exception for national security related matters. It requires that, in general,

each agency must, among other things: (1) propose or adopt a regulation only upon a **reasoned determination** that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify); (2) **tailor its regulations** to impose the **least burden** on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the **costs of cumulative regulations**; (3) select, in choosing among alternative regulatory approaches, those approaches that **maximize net benefits** (including potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity); (4) to the extent feasible, specify **performance objectives**, rather than specifying the behavior or manner of compliance that regulated entities must adopt; and (5) identify and assess **available alternatives** to direct regulation, including providing economic incentives to encourage the desired behavior, such as user fees or marketable permits, or providing information upon which choices can be made by the public.³

This is the “gold standard” to which BIS should aspire. Doing so requires soliciting comments on potential costs and benefits, precisely as BIS has done in the Proposed Rule — but also that BIS issue a report on its analysis along with any modifications to the Proposed Rule that may be required by that analysis *before* issuing a final rule. Jumping straight to a final rule without giving the public an additional opportunity to comment on both BIS’s cost-benefit analysis and the revised rules would render any cost-benefit analysis the agency might perform essentially perfunctory: only further public comment can ensure that this analysis is adequately rigorous and that BIS further revise its rules as necessary.

Cybersecurity is simply too important for BIS to rush this rulemaking. We look forward to providing additional comment on BIS’s revised rules — and to seeing BIS’s report on the costs and benefits of its proposal.

³ Exec. Order No. 13563, 76 C.F.R. 14 (2011) (emphasis added).

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-qnjc
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0190

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anonymous Anonymous

General Comment

Too broad and too vague. This is going to have a chilling effect on legitimate security researchers who keep us safe.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-nzyb
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0191

Comment on FR Doc # 2015-11642

Submitter Information

Name: Dan Kaminsky

Address:

178 Bluxome St.

#510

San Francisco, 94107

Email: dan@doxpara.com

Phone: 4089338195

Organization: White Ops

General Comment

Please see attachment for my formal commentary. If there is any issue parsing the file, please contact me.

Yours Truly,

Dan Kaminsky

Chief Scientist

White Ops

Attachments

bis_comments

To Whom It May Concern:

My name is Dan Kaminsky. I am the Chief Scientist and Co-Founder of White Ops, a computer security firm based in New York and San Francisco. For over fifteen years, I have been on a mission to make the Internet safe. After working extensively with Cisco, Avaya, and Microsoft, I discovered – and with the help of an international cadre of engineers, remediated – a major flaw in the core design of the Internet. Since then, I have been named one of seven Recovery Key Shareholders to the Internet's Domain Name System – I am the American of this group. Furthermore, I was part of a group of Internet engineers that critiqued the SOPA and PIPA bills that sought to regulate the Internet in ways that, as we determined, would cause detriment to the network global business and society now depends upon.

I provide this information so that there may be some context to my words. I am focused on protecting the Internet – for users, for business (large and small), for society. I understand the impetus behind creating a regulatory regime around computer security – it's ugly out there, and I feel the drive every day to do something.

My commentary to you is this: These policies are too soon, too much, and far, far too unilateral.

By too soon: It might seem strange for a "White Hat Hacker" known to focus on defense, to come to the defense of what may seem to be purely offensive technology. The reality is that we are still in the process of learning how to make secure networks. *A lot of people are going to have to learn how things break, if we are to have any hope of making things that survive attack.* As we tend to say, defense minus offense is compliance. *Existing compliance regimes have not generated sufficiently resilient networks.* When I say these regulations are too soon, I am specifically stating that we are at a turning point – we can't go on with the cyber equivalent of our bridges collapsing, our cities burning, our basic services subject to the whims of random or organized miscreants.

These proposed regulations will choke off the supply of those knowledgeable to build better. We aren't at the phase where we know what fire codes to specify. You're at the phase where you're tightly regulating chemistry and material science, just as we *really really* need people to understand how things actually fail in the real world.

I have seen what engineers build when they have no concrete security knowledge.

It burns.

There was an astonishing situation in Iraq some years ago. Drones were using completely unencrypted video feeds – to the point where, at least as was reported, a simple satellite dish was enough to pick up the feed. Why wasn't encryption used? Ah, that would require compliance with complex regulations...unsafe could fly now.

The scenario with Hacking Team has also come up as an example. As fellow researcher Dan Guido has noted, Hacking Team had all its permits, all its licenses, all its paperwork well in order. Those attackers are not suppressed by this proposed regime; they are instead protected, even coddled. There is a new generation of security technology really taking shape -- technology driven by passionate engineers out to disrupt and defend in new and genuinely exciting ways.

Now is not the time to be injecting risk and regulation into their engineering and their businesses. The Federal Government has much more supportive things it can do, to deal with the pernicious cyber threat to global stability.

It's not about what code shouldn't be written, shouldn't be sold, shouldn't be understood. It is too soon for all that, and to be blunt, you're only shooting us in the foot. *Help us build more.*

Others (particularly Sergey Bratus) have written extensively about the flaws in your proposed regulations. My sense is that they bear too much of the mark of their source – they come from the world of export control and diplomacy. This makes sense when the means of production are limited to Nation States; the reality is that offensive knowledge can and regularly is reproduced by teenagers. Repeatedly, we have seen significant attacks ultimately attribute to youth. When the biggest attackers can survive your licensure, and the smallest can evade your focus, you only end up hamstringing legitimate business, academic, and engineering interests.

There has been some positive work on making explicit safe harbors. This, I support. Computer Security work in the public view can be a bit of a high wire act at times. You really do sometimes need to put it all out on the line and hope nobody gets too angry (or if they do, you will get enough support to survive complaint). Ultimately the security research community has won enough of these fights that once unthinkable changes – like ISO standardization for handling vulnerability disclosure! – are normalizing. I encourage your continued work making explicit behaviors that create affirmative safe harbors.

The pushback received may feel unexpected – I understand you're seriously trying to help, and you believe you've had the advice of all the necessary stakeholders. The reality is that there's just a lot more going on here – significant business interests, major engineering movements, and yes, a society that is looking for more protection than we have today. Please, continue your efforts to make the Internet safer. But limiting knowledge of how to do that, is not in my professional opinion the right place to start.

Yours Truly,

Dan Kaminsky
Chief Scientist
White Ops

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3f-nl07
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0192

Comment on FR Doc # 2015-11642

Submitter Information

Name: Frank Martinjak

Address:

TX,

General Comment

I am an information security researcher. My efforts have worked to secure systems and protect people. Please don't turn me into a criminal.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-ytuk
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0193

Comment on FR Doc # 2015-11642

Submitter Information

Name: Carl Mehner

Address:

San Antonio, 78254

Email: c+reg@cem.me

Organization: cem.me

General Comment

Dearest Regulations.gov,

I am a security researcher that uses and creates security tools which are useful for finding vulnerabilities in computer software and systems.

This arrangement is too broad and too vague, would require more tax payer money to review/issue licenses that would be required for the software that is under the proposed agreement, proposes spurious license that appear to be required to even report a security vulnerability, creates a 'chilling effect' on vulnerability research that would be detrimental to the security research community as a whole, and restrict sharing that is crucial to the effective operation of global information security governance.

The conclusion here is to roll this back, not to further muddy the waters and do it as soon as possible (during the meeting this December). There is no way to tell 'bad actors' from the good, and as such there ought to be no restriction on who is able to use which ever tools they so happen to use. In light of this, you must do your duty to our national security and remove software from the Wassenaar controls. Code is not a weapon, declaring it as such will underpin

the security research community and create a void in our ability to have a unified front against these 'bad actors' that seek to undermine our security without creating a net-good.

Forcing companies and researchers to apply for the necessary licenses and answer the necessary questions (paragraph (z) to Supplement No. 2 to part 748) would create an undue burden on our companies and our citizens.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-knml
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0194

Comment on FR Doc # 2015-11642

Submitter Information

Name: Corey Thuen

Email: thuen@digitalbond.com

Organization: Digital Bond Labs

General Comment

I work in cybersecurity specializing in critical infrastructure systems. Please do not go forward with this as it has negative consequences that prevent people like me, the GOOD guys, from effectively working to secure our infrastructure against actual bad people.

Do not do this.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-cjrf
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0195

Comment on FR Doc # 2015-11642

Submitter Information

Name: Anton Schieffer

General Comment

This proposed language is too restrictive and harms information security researchers. At least, that's what it appears -- the actual language is quite open-ended, so it's hard to know with much certainty. It appears to restrict research which is highly unlikely to be deterred, and would give the United States an unfair strategic disadvantage. The proposed language criminalizes those who attempt to make the Internet a more secure place. Information security research creates a safer Internet, and arbitrarily restricting its use would likely create unintended consequences. Please reconsider this language and consult more thoroughly with the information security community before seriously considering bills like this.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-kp2m
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0196

Comment on FR Doc # 2015-11642

Submitter Information

Name: David Longenecker

Address:

Austin, TX,

Email: dnlongen@gmail.com

Organization: SecurityForRealPeople.com

General Comment

I frequently write about malware, spam, credit card fraud, and various computer crimes. In my and others' writing it may seem as though there is an easy distinction between the legitimate and the malicious. The reality is, the world of online security is not always black and white. More often, it is filled with shades of grey.

With the BIS rules regarding the Wassenaar Arrangement there is a danger that well-meaning legislators that don't understand what they are legislating could cause more harm than good. The BIS proposes to restrict transfer of software and knowledge related to intrusion systems, penetration testing products, and IP network communications surveillance systems or equipment.

I am not an "elite hacker" by any definition, but do research into vulnerabilities in products that I use. Under certain interpretations of the BIS proposal, several of my projects and vulnerability disclosures could needlessly fall under restrictions. Attached are details.

Security research is shrouded in shades of grey. Black and white laws with no room for interpretation, or no exemption for good-faith research and sharing, risk squashing an industry

of good guys. The research we do - often on our own time with no expectation of being paid - results in better security for everyone. The bad guys will continue researching and exploiting vulnerabilities regardless of the law. My "hacker" peers and I just want to find and fix flaws first. Don't discourage us.

Attachments

Wassenaar

I frequently write about malware, spam, credit card fraud, and various computer crimes. In my and others' writing it may seem as though there is an easy distinction between the legitimate and the malicious. The reality is, the world of online security is not always black and white. More often, it is filled with shades of grey.

The same behavior may be perfectly legitimate in one context, and purely criminal in another. The same program or tool can be used for benevolent purposes by one person, and for malicious gain by another. In fact one person may use technology tools for good by day, and for evil by night: Brian Krebs wrote in his book *Spam Nation* the tale of Pavel Vrublevsky, a Russian who simultaneously ran a widespread pharmaceutical spam program and served as chairman for the anti-spam working group in the Russian Ministry of Telecom.

With the BIS rules regarding the Wassenaar Arrangement there is a danger that well-meaning legislators that don't understand what they are legislating could cause more harm than good. The BIS proposes to restrict transfer of software and knowledge related to intrusion systems, penetration testing products, and IP network communications surveillance systems or equipment.

I am not an "elite hacker" by any definition, but do research into vulnerabilities in products that I use. Under certain interpretations of the BIS proposal, several of my projects and vulnerability disclosures could needlessly fall under restrictions.

About a year ago, I found that my wireless router was not updated to the latest available firmware, even though the update button said it was up-to-date. Being a curious soul, I set out to find out why. Eventually I discovered that my router relied on a file stored at the manufacturer's website, which listed the latest firmware version for every router model; that file had not been updated, so as far as my router knew, it had the latest version.

My research was completely aboveboard, with no malicious intent nor malicious use. In fact, that research led to an informal relationship with the product team at this manufacturer such that I've been able to beta test several new products and recommend changes to make them more secure upon public release. In fact, I have discovered a few more serious flaws, which the company fixed before I published my research. Under the proposed law though, I accessed the website in a manner that was not intended by the manufacturer, and thus exceeded the intended authorization. My blog posts describing the flaws could enable a malicious hacker to gain access to devices where the owner has not updated to the fixed firmware. My beneficial research - which has resulted in more secure routers used in hundreds of thousands of homes and small businesses - could have instead been interpreted as proprietary research into vulnerabilities and exploitation of network-capable devices.

As another example, I use a variety of software and devices to protect my home network from viruses, malware, and attacks. A recent addition was an IDS, or intrusion detection system, using open-source Snort software on a Raspberry Pi running Kali Linux. I wrote some custom rules to detect undesired activity by looking at the responses OpenDNS gave to domain name queries. OpenDNS is like a smart phone book: for most websites it responds with the correct network address, but for known undesirable sites (whether they be malicious, or blocked by our family policy), it instead responds with the address of a page that says "you don't really want to go here."

Shortly after turning on the system, I noticed that my teenage son's laptop was frequently making DNS queries that triggered alerts - at a rate orders of magnitude more frequent than any other devices on the network. On investigating, almost all of these alerts were for requests for advertising domains. The culprit was two browser "helpers" that had been installed on his computer - one known as "Jollywallet" and the other as "LPT Monetizer." Both are programs that hook into a web browser and display advertisements, presumably to earn money for those controlling the ad network. More advertising impressions equal more revenue.

Why did my anti-virus program not detect and block these programs? Strictly speaking, they are not malware. They don't steal passwords or break into bank accounts. They don't delete files or destroy hard drives. They don't seek out other computers to infect, or databases to hack. Somewhere along the line, they probably came as a hidden "benefit" of a game or other program my son intentionally installed.

The implementation of Snort to inspect DNS responses, and my subsequent description of the project and release of my proprietary Snort rules to the public could be interpreted as a communication with intrusion products.

Google, Cisco, and others with a legion of legal counsel have written their own comments to the proposed rules. I and many of my peers have no such counsel: we are individuals doing our part to make the Internet a safer place, often by researching vulnerabilities and exploits -- and ways to counter such exploits. When even a legion of legal experts cannot be certain whether a given activity falls under export controls, folks such as myself have no chance of understanding the ins and outs of the rules. Many such as myself are likely to stop such research rather than risk running afoul of federal laws. And when the good guys quit, all that will be left will be the criminal hackers.

Security research is shrouded in shades of grey. Black and white laws with no room for interpretation, or no exemption for good-faith research and sharing, risk squashing an industry of good guys. The research we do - often on our own time with no expectation of being paid - results in better security for everyone. The bad guys will continue researching and exploiting vulnerabilities regardless of the law. My "hacker" peers and I just want to find and fix flaws first. Don't discourage us.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-45z8
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0197

Comment on FR Doc # 2015-11642

Submitter Information

Name: Wayne Baisley

Address:

IL, 60540

General Comment

This proposal will primarily burden and criminalize legitimate security professionals and communications developers, and do so in the most vague and arbitrary ways possible. No tool, from a simple hammer to the most advanced aircraft, has ever been made that could not be used for bad purposes. Attempts to regulate communications products into safety, cannot succeed without doing immense damage to the providers and to society at large. And a great many features of modern communications systems was never intended, per se, but grew as hackers, experimenters, and visionaries built on and modified existing facilities. This agreement doesn't appear to make any provision for such possibilities. It is as an inevitable consequence, antithetical to American values.

These are not features that will "buff out." I sincerely and wholeheartedly request that this agreement be rejected in toto, and a different approach be taken, as particular well-defined and targeted may be identified.

Thank you.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-z7eu
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0198

Comment on FR Doc # 2015-11642

Submitter Information

Name: Ryan Castellucci

Address:

PO Box 1431

Palo Alto, CA, 94302

General Comment

I've been doing cybersecurity professionally for about six years now. I've spoken at conferences on cybersecurity. I've read through the regulations twice, and I'm still not entirely sure what exactly they mean.

My concern is that a lot of technology these regulations intend to restrict is inherently multi-use. Many tools can be used both to build and destroy, and that's just as true for cybersecurity tools as it is for more traditional ones. We don't ban hammers because they could be used to beat someone.

The tools I use every day can be used for "intrusion". Though I intend it to be used for good, some of the software I write could be used for "intrusion". Your regulations have dangerous potential to criminalize the entire security industry, leaving the entire world, but especially the United States, more vulnerable. The real bad guys are already underground, and won't be hindered in the slightest.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-zhhu
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0199

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jose Fernandez

Address:

706 Crawfords Knoll Ct

Odenton, 21113

Email: info@compsecdirect.com

Phone: 4433450503

General Comment

See attached file(s)

Attachments

Wassenaar Agreement CompSecDirect

COMPSEC DIRECT

706 CRAWFORDS KNOLL CT, ODENTON, MD, 21113 443-345-0503 INFO@COMPSECDIRECT.COM

This letter is in reference to the Wassenaar Arrangement (WA) 2013 request for comments via the Bureau of Industry and Security (BIS) BIS-2015-0011. Our company is deeply concerned with the vocabulary and intent that the proposed modifications to WA includes in these revisions. We are a small company comprised of security experts and researchers. Our staff includes personnel that conducted some form of vulnerability analysis and cyber operations within the Department of Defense under the rules of regulations of the United States (US) government. Based on our experience with Federal regulations, we feel the proposed revisions to WA essentially creates numerous foreseeable problems to individuals inside the Information Security community domestically and abroad since the WA already includes numerous problems.

As a computer security company, we understand the need for some form of restriction for items already covered within WA; such as weapons and other tangible assets. Using WA to control encryption created or funded by the US government or US companies was inevitably doomed to fail as society became more interconnected and sharing previously guarded cryptologic controls covered under WA became impractical and impossible to effectively enforce. The WA revisions represent a noble, yet flawed attempt by US lawmakers and policy decision makers to attempt to rein in this uncontrollable problem (ECCN 5A001.j, 4A005, 4D004). Encryption, as opposed to destructive devices and weapons, is intangible and simpler to conceal than before. Using WA between countries seems more like a gentleman's agreement to respect each other's intellectual property as a matter of convenience. The revisions to WA propose licensing fees and dues which creates a market place of elitism where only well financed corporations in the Information Security industry can play (ECCN 4D001). These revisions, as they are currently worded, will limit innovation and the development of small companies within the US (§ 742.6(b)). The ENC Encryption Request Coordinator cannot feasibly accomplish this undertaking in our opinion.

We are aware that the US government does not want companies either US based or incorporated within the US to simply export encryption to countries with strained diplomatic ties; however this is already covered in the current WA as it is written. The revisions attempt to include a broad range of security applications, programs and high level concepts. In this case, the vocabulary is generalized and is the equivalent of attempting to regulate the dissemination of a tool (ECCN 4A005). As an Information Security professional, many of the terms placed into restriction via WA 2013 are the tools we use to help grow and secure our customers networks. These revisions are similar to attempting to regulate a carpenter's hammer and nails and a plumbers solder torch. The WA revisions also serve as a punitive basis when we notify customers in the private and public sector of potential vulnerabilities and data breach. Instead of allowing Information Security companies, Information Security professionals and Information Security students the ability to notify and help and organizations improve current security controls and practices; you are creating a legal basis which companies and organizations can leverage against individuals under the guise of protecting the priorities of the few while violating the constitutional right of freedom of speech (ECCN 5A001.j, ECCNs 4A005, 4D004, 4E001, 5A001, 5A002, 5D002 and 5E002). Encryption, and the ability to decrypt, is now commonly found in many of the security tools the WA 2013 revisions attempts to limit. This also limits the effectiveness of how well future Information Security professionals and companies conduct business.

If individuals and companies like us cannot divulge or notify companies that their customer and financial information can be exposed or is exposed, where will it end? Will the use of common security tools and techniques inside the Information Security community be impacted by the current draft of WA 2013? Yes, it will. Because of this, the BIS needs to revise the broad vocabulary used and listen to the overwhelming voices of reason that have taken a stand against the current draft of WA 2013.

Attentively,

Jose Fernandez
President CompSec Direct
Information Security Researcher

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-7h09
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0200

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael James

Address:

5175 Arnold Rd

Lexington, NC, 27295

Email: phra95w17ch@gmail.com

Phone: 3368470782

General Comment

A lot of people working in the Information Security sector are doing good, thankless work. But all of us do this not only because we love what we do, but who we do it for, which is everyone, everywhere. Our fight is hard enough as it is, so please, for the love of our country, don't make it any more difficult!

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-za2a
Comments Due: July 20, 2015
Submission Type: Web

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0201

Comment on FR Doc # 2015-11642

Submitter Information

Name: Dino Dai Zovi

Address:

228 Park Ave S

#21664

New York, NY, 10003

Email: ddz@theta44.org

Phone: 19173460538

General Comment

See attached file(s)

Attachments

RIN_0694-AG49_web

Dino Dai Zovi

✉ ddz@theta44.org

🌐 www.theta44.org

July 20, 2015

Catherine Wheeler

Director

Regulatory Policy Division

Bureau of Industry and Security

Room 2099B

U.S. Department of Commerce

14th and Pennsylvania Avenue, N.W.

Washington, DC 20230

Dear Director Wheeler:

I am submitting the following comments for your consideration on the proposed implementation of the Wassenaar Arrangement controls on Intrusion and Surveillance Items (aka "cybersecurity items") referenced under Docket ID BIS-2015-001 and RIN 0694-AG49. I submit these comments in my personal capacity; they are not meant to represent the view of past or current employers.

I am a cybersecurity professional with a career spanning roles as a member of the Information Design Assurance Red Team at Sandia National Laboratories (www.sandia.gov) where I performed adversarial cybersecurity assessments to presently leading Mobile Security at Square (www.squareup.com) where I manage the engineering of systems that secure payments and commerce on mobile platforms. My early interest in cybersecurity was driven by a fascination with memory corruption-based security vulnerabilities, and my research into it launched my career in cybersecurity. The potential regulation of this field of research is a serious concern to me and especially the adverse effects the proposed regulations will have on it. Of primary concern is the addition to ECCN 4E001.a of "technology required for the development of intrusion software," its inclusion of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices," and especially the restrictions on "deemed exports" of it.

My research into memory corruption-based security vulnerabilities and their exploitation on computers and network-capable devices is what sparked my interest and self-study into cybersecurity. I learned about them from information freely published on the Internet by the international security community, and I have studied them extensively through my own research while in school and throughout my career. I first presented my research into the exploitation of vulnerabilities on SPARC-based systems at the DEFCON 8 conference in July 2000. This presentation was attended by some of my future colleagues on the Information Design Assurance Red Team (IDART) at Sandia National Laboratories, where I began my career in cybersecurity. My personal research and its contributions to my early career would have been significantly hampered had the "deemed exports" of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices" been restricted at that time by the various home countries of the international security research community.

I now lead the Mobile Security team at Square (www.squareup.com). In order to design and produce more secure products, we must understand the limitations of the technology platforms they are built

upon. We gain insight into this by performing our own vulnerability and exploitation research into these platforms. This research guides us and helps us design proactive defenses and exploitation mitigation features into our products. Our products, and the security of our sellers' businesses, depend on the security of the mobile platforms that they are built upon. We are able to ensure the security of our products through these proactive defenses guided by our own research. Our team includes non-U.S. persons (i.e. those employed through a visa rather than having permanent resident status) and communicating that research to them in order it to help them design more secure products could, under the current proposal, be interpreted to be a "deemed export" of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

I am also presently a Hacker-in-Residence at NYU's Polytechnic School of Engineering (engineering.nyu.edu). In this role, I utilize my expertise and industry connections to assist the department's students and faculty in education, events, and outreach. As a part of this, I have contributed educational materials that demonstrate how to evade "protective countermeasures" such as DEP and ASLR. These materials were created for open trainings in the U.S. and Canada but are not otherwise publicly available. This material is still being taught to both on-campus and e-learning students in the Penetration Testing and Vulnerability Analysis (CS-GY 6573) course. Like most engineering schools in this country, the student base includes many international students on student visas as well as remote e-learning international students. Under the current proposal, this course could also be considered a "deemed export" of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

As a now-prominent member of the international security research community, I am in frequent communication with my network of peers and colleagues around the world. It has long been a part of the culture of this community to share personal research on vulnerabilities and exploitation amongst each other. This research may or may not result in future published work (i.e. papers, books, conference presentations) but is shared privately in order to foster collaboration and understanding. This non-commercial collaboration that had long preceded our employment in cybersecurity has benefited our careers and our work for our employers significantly. Under the proposed rules, any personal research that I may now perform in my spare time and completely independent of any past or present employment would not likely be able to be shared among this community as it would become a "deemed export" of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

The proposed restrictions on surveillance equipment restricts the regulations to classes of equipment that require significant time and capital investment towards end products that are unambiguously designed for mass surveillance. In contrast to this, the proposed regulations on "technology required for the development of intrusion software" are unnecessarily broad and cover spare-time activities among hobbyists at "hackerspaces" around the country. While much of the security research performed by these hobbyists eventually results in published work and vulnerability disclosures, sharing it beforehand with any non-U.S. members of the hackerspace would, under the proposed rules, be considered a "deemed export" of "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

Significantly hampering collaboration on security research or even merely creating a chilling effect upon that collaboration will have a definite impact on the growth and nurturing of the cybersecurity

workforce needed by U.S.-based companies, institutions, and government agencies. The present scarcity of capable cybersecurity professionals needed to secure our technologically dependent economy, society, and government will be exacerbated by the proposed rules and growing the size and capability of that workforce will have a greater positive effect on our national security and prosperity than the controls proposed by these regulations.

For all of these reasons, I urge revision of the proposed rules restricting “technology required for the development of intrusion software,” to exclude the “proprietary research on the vulnerabilities and exploitation of computers and network-capable devices” and especially the “deemed exports” thereof.

Respectfully,

A handwritten signature in black ink, appearing to read 'Dino Dai Zovi', with a long horizontal flourish extending to the right.

Dino Dai Zovi

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-zj4e
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0202

Comment on FR Doc # 2015-11642

Submitter Information

Name: Douglas Twitchell

Address:

Campus box 5150

Normal, IL, 61790

Organization: Illinois State University

General Comment

The proposed rules will actually make us less secure by restricting those who are doing the most to secure our information.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-csoe
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0203

Comment on FR Doc # 2015-11642

Submitter Information

Name: Michael Toecker

Address:

5360 Pershing Ave

Unit 1B

St. Louis, 63112

Email: michael.toecker@gmail.com

Phone: 6159486954

Organization: self

General Comment

I work in the computer security industry, and have done so for 10 years of my life. This industry is a force for good, we study and evaluate computer security problems and attempt to eliminate them. We pull together to defend systems, and to do this we must point out weaknesses.

The only way to do this is to use the same tools that an attacker might use. I am concerned that my ability to create tools and techniques that ultimately serve the good will become illegal, and I will be blind to what those who do not abide by the law.

I could say that this is similar to research on smallpox, and measles... Evils that humankind has all but eradicated. I could say that despite the fact we have all but eradicated them, we continue to keep them in labs to study how they propagate and use them to develop more effective vaccination and immunization technologies. I could say that, but viruses do not THINK. They do not PLAN, they do not PLOT.

Attackers DO think. They DO plan, and they DO plot. They develop and use tools like what you would make illegal. Attackers are perfectly capable of developing these tools in isolation far away from laws and regulations, to do harm to citizens and allies. They can trade them in darknets, which will never be fully policed.

I intend to forge shields from their swords, helmets from their arrowheads, and walls from their bulldozers. Do not deny me, and my fellows, the capability to do this. It would be folly.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-bqcd
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0204

Comment on FR Doc # 2015-11642

Submitter Information

Name: Christina Wuest

Address:

6521 Spring Lark
San Antonio, TX, 78249

Email: tina+frgov@wuest.me

Phone: 2102417630

General Comment

This will outlaw legitimate security research and collaboration while failing to hinder any criminal, terrorist or other existential threat to the safety of law abiding citizens in the US or elsewhere. The result is that the United States will no longer be a safe place to work for good, while the US will not become meaningfully more dangerous for those seeking to do harm.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-2g80
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0205

Comment on FR Doc # 2015-11642

Submitter Information

Name: Jesse Lyon

General Comment

This whole argument is very similar to the gun control debate. Outlaw guns, gun crime will go down correct? Based upon the atrocities in gun free zones such as what happened in Chattanooga this week, Sandy Hook a couple years back, and Chicago almost daily we know this hopeful assumption to be patently false. If you outlaw guns, law abiding citizens will no longer have the means to protect themselves. This is almost an exact analogy of the information security field. The tools we use daily to audit our clients or to work with others in the community to develop stronger methods of cryptography, harden network infrastructure, or keep your coffee pot from being taken over, could just as easily be used to break into someone else's network. The fact that these tools are readily available open the door to the next generation of talent learning how to protect our country from cyber threats. Time, and time again we have seen controls put into place over things such as this, things that certain threat actors can bypass the law and attain much easier than law abiding citizens. We in information security have a much keener view of just how dangerous the world is around us from a cyber threat perspective, and it is we who are clamoring to have these draconian rules dropped from pending legislation. By outlawing critical tools and knowledge needed to mitigate threats, the government effectively stifles security professionals from doing their jobs, putting the world in far greater jeopardy. Give us the tools we need to fight the threats we face to day, to better secure the world tomorrow.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 20, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k3e-uqdw
Comments Due: July 20, 2015
Submission Type: API

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0206

Comment on FR Doc # 2015-11642

Submitter Information

Name: William Showalter

Address:

9970 E Birch Forest Cir

Palmer, AK, 99645

Email: williamshowalter@gmail.com

Phone: 9079821424

General Comment

Restricting the ability to legally research security topics does nothing to prevent those with malicious intent from discovering, creating, and using exploits. In fact, it helps the malicious parties by restricting the availability of knowledge to those who are designing/improving systems and driving that knowledge into clandestine rings.

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-gst1
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0207

RIN 0694-AG49 EDAC Response

Submitter Information

General Comment

See attached

Attachments

RIN 0694-AG49 EDAC Response



July 17, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49) Published in 80 Fed Reg 28853 on May 20, 2015

Dear Sir or Madam:

The Electronic Design Automation Consortium (EDAC) is the international association of companies developing EDA tools and services that enable engineers to create the world's electronic products. The EDA Industry provides the critical technology and infrastructure to design electronics that enable the Information Age, including communications, computers, space technology, medical and industrial equipment, and consumer electronics. EDAC's Export Committee comprises compliance professionals dedicated to providing guidance concerning regulations affecting our industry.

Thank you for the opportunity to provide comments on the proposed rules on Intrusion and Surveillance Items.

The EDAC Export Committee is concerned that as proposed, the regulations are open to interpretations that could result in the unintended control and classification of software used for preventing attacks and improving software security under the new restricted intrusion software categories. We recommend adding a note or Commodity Interpretation to specifically exclude software designed for defensive purposes from the 4D004 and 4D005 classifications, and to exclude certain defensive technology from the 4E004 and 4E005 classifications.

Without these specific exclusions EDAC member companies are likely to be confused about the applicability of the new categories. This will result in large numbers of unnecessary export license requests.

Where Electronics Begins™

Electronic Design Automation Consortium · 3081 Zanker Road · San Jose, CA 95134 · www.edac.org
main 408-287-EDAC (3322) · fax 408-317-EDAC (3322)

Introducing ambiguity and doubt regarding the applicability of the new regulations will have another significant negative impact: The adoption and use of legitimate defensive software will be slowed, making it more difficult to prevent attacks and malicious hacking that threatens US business and industry. Reducing the availability of defensive software products through the application of overly broad controls will increase the risks that EDAC members, and many businesses face in trying to safeguard our own networks and products.

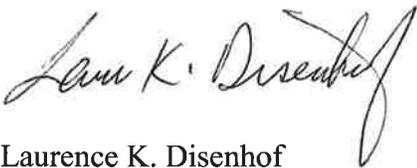
Recommended language for a note or Commodity Interpretation is:

Software specifically designed for defensive purposes or to improve software performance or quality is excluded from 4D004 and 4D005. Excluded purposes are: software testing, software or design verification, error detection, security analysis, vulnerability detection, network penetration testing, and software or network performance monitoring.

We respectfully request that BIS postpone implementation of the regulation until the scope has been clarified and narrowed, and encourage the U.S. Government to work with its Wassenaar partners to similarly clarify the regulation adopted at the 2014 Plenary.

On behalf of EDAC's Export Committee, I thank you for the opportunity to provide comments on these proposed rules.

Sincerely,



Laurence K. Disenhof
Chair, EDAC Export Committee

Where Electronics Begins™

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-fm7o
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0208

RIN 0694-AG49 Congressional Wassenaar Comments Signed

Submitter Information

General Comment

See attached

Attachments

RIN 0694-AG49 Congressional Wassenaar Comments Signed

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-h6jm
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0209

Comments for Coalition for Responsible Cybersecurity - RIN 0694-AG49 This replaces BIS-2015-011-Draft-0172

Submitter Information

General Comment

See attached

Attachments

Comments for Coalition for Responsible Cybersecurity - RIN 0694-AG49

Meredith Rathbone
202 429 6437
mrathbone@steptoe.com



1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

July 20, 2015

Via e-mail

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20230
publiccomments@bis.doc.gov

Attn: Catherine Wheeler, Director, Information Technology Controls Division

**Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation:
Intrusion and Surveillance Items**

**Reference: BIS-2015-0011
RIN 0694-AG49**

Dear Ms. Wheeler:

These comments are submitted on behalf of the Coalition for Responsible Cybersecurity (the "Coalition") to express the Coalition's concerns with the BIS proposed rule *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28,853 (May 20, 2015) ("the proposed rule"). The Coalition's mission is to ensure that U.S. export control regulations do not negatively impact the effectiveness of U.S. cybersecurity or prevent the United States from maintaining its leadership role in that sector. The Coalition is representative of a broad range of companies, and includes Ionic Security Inc., Symantec Corporation, FireEye, Inc., Synack, Inc., Trail of Bits, Inc., Global Velocity, Inc., and WhiteHat Security.

U.S. companies design, test, develop, and field some of the world's leading technologies in critical areas such as network monitoring, penetration testing and encryption. Development of these cutting-edge defensive technologies relies on the ability to conduct unfettered research into vulnerabilities (including novel, zero-day vulnerabilities), as well as reverse engineering cyber threats and other basic methods of cybersecurity research. However, robust research and

development are only feasible when there is an open, global market for the products. If U.S.-origin technology becomes “tainted” by burdensome export control restrictions, U.S. companies will lose their leadership position, to the detriment of all the companies, organizations, governments and individuals that rely on U.S. cybersecurity to defend against malicious attacks.

U.S. companies “export” these defensive technologies virtually every second of every day. Imposing the far-reaching licensing requirements that BIS has proposed would harm not only U.S. cybersecurity companies, but would harm cybersecurity itself. The Coalition is committed to helping the U.S. government ensure that its export control regulations are informed by the realities of the cybersecurity world and do not inadvertently restrict beneficial activity or miss the mark in attempting to control malicious activity. It is also important that U.S. export controls remain in line with, and not needlessly more restrictive than, those of its major trading partners and technological competitors. Otherwise, U.S. cybersecurity leadership and expertise will weaken, causing the United States to lose its strategic edge and its world-leading contributions to this arena, while the cybersecurity markets continue to strengthen in countries that are not subject to such harsh restrictions.

The Coalition has done its best to craft useful and detailed comments in the short period of time that BIS has allowed. However, the Coalition is unable to raise all of the concerns implicated by this sweeping regulation in this initial round of comments. Due to the complicated nature of this proposed rule and its effects on industry, the Coalition believes that a second proposed rule and round of comments is necessary. The current proposed rule as drafted would have a devastating effect on U.S. cybersecurity and must be fundamentally restructured. We discuss in more detail in Section VII.A.3, below, what a productive subsequent proposed rule might look like.

I. INTRODUCTION

The proposed rule would achieve the exact opposite of what the Wassenaar group intended: rather than effectively restricting trade in malicious items, it will primarily control the defensive technologies that law-abiding organizations rely on to protect themselves against those malicious items. Many of the Coalition’s concerns with the proposed rule focus on its use of ambiguous language and overbroad definitions that capture defensive tools and standard software development techniques that apply even outside the security sphere. In its Frequently Asked Questions (“FAQs”) on the proposed rule, BIS itself expressed the difficulty it faced in defining some of the terms, such as “carrier class”.¹ Terms like “rootkit” and “zero-day” are used in the proposed rule with no definitions, even though they have more than one accepted meaning in the cybersecurity community. The definitions that are provided, such as for “intrusion software,” are overbroad and unworkable. They cover a wide range of cybersecurity products that BIS likely did not intend to target.

¹ See, e.g., BIS, Frequently Asked Questions, Intrusion and Surveillance Items (“FAQs”) #14, <https://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>.

BIS itself has recognized that the proposed rule captures some defensive products and methods, such as network penetration testing.² That the proposed rule captures penetration testing should not be taken lightly. Penetration testing is a standard operational need to maintain the security of electronic systems; in fact, penetration testing is required by numerous industry standards and regulations.³ As currently written, the rule would cover numerous other defensive products in addition to penetration testing, because the products security professionals use to add new security features and patches are frequently technically indistinguishable from those used by attackers to alter programs in malicious ways. There are very few characteristics or behaviors that can even be potentially considered unique to malicious tools, and even screening for these malicious characteristics often brings up false positives for security software, demonstrating that there are probably no characteristics that are exclusively malicious. While BIS has recognized the difficulty of distinguishing between offensive and defensive products, it has not succeeded in implementing an effective distinction. That is a critical shortcoming that calls for more time to allow the government to consider how to craft a regulation in this area that would achieve its stated objectives without unnecessary collateral damage. Again, we provide some preliminary suggestions for how to get started on this effort in Section VII.A.3, below.

The proposed rule makes no effort to distinguish between items that assist in interfering with or extracting data from *malicious* programs (in order to defend against them) and those that maliciously interfere with *legitimate* programs (as a means of attack). Many security tools use technology that implements, executes, or monitors malware and extracts data from that malware for defensive purposes. Such tools need reliable ways to be generated, operated, and delivered, all of which would be unduly restricted under the proposed rule. Similarly, many benign products meant to patch systems or programs, or add capabilities that the authors did not originally contemplate, do so by interacting with and manipulating the program in ways that would be captured under the proposed definition of “intrusion software.” The cybersecurity community is global and their defensive efforts occur in real time and often depend on collaboration across borders. These controls would greatly complicate these collaborative efforts and access to legitimate software tools. But the proposed rule is unlikely to stop malicious actors from sharing and using their products because these actors often operate outside the reach of U.S. regulatory power. Additionally, even though other Wassenaar countries have used much of the same overbroad and fundamentally problematic language from the December 2013 plenary, this proposed rule controls an even wider range of items than Wassenaar and other countries’ implementing rules, including differences in the implementation of the General Software Note and General Technology Note.

² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28,854 (stating that the new controls will “include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices”).

³ See, e.g., Federal Information Security Management Act (FISMA) of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3544(b)(5); see also *Technical Guide to Information Security Testing and Assessment*, U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-115 (September 2008); *Penetration Test Guidance*, Federal Risk and Authorization Management Program (FedRAMP), Version 1.0.1 (July 6, 2015). See generally, Section V, below.

From an overall perspective, the proposed rule is unworkable because the language that was adopted in December 2013 by Wassenaar is fundamentally flawed. Ideally, rather than try to adopt this language through regulation in a sweeping and harmful way, the U.S. must return to Wassenaar to change this language. Because of the unique nature of the cybersecurity industry, which depends on rapid information sharing among an international community of professionals, no traditional export control licensing policies can solve the fundamental problems in the proposed rule. These issues likely stem from the adoption of the Wassenaar language without any industry input. Tellingly, the overwhelming majority of the cybersecurity industry is in the United States, while the Wassenaar rule was proposed by a European country without seeking feedback from U.S. industry. Now that U.S. industry's input is being heard, it is unfortunately—but inescapably—necessary to go back to the drawing board. Given the likely timeline for revisiting this issue at Wassenaar, and the timeline for a second notice and comment period, we believe that returning to Wassenaar will not significantly delay the United States' implementation of a cybersecurity rule. Specifically, due to the significant problems with the current proposal, and the need for a second round of comments to get industry input on any revisions, this rule is unlikely to be anywhere near finalization by February 2016, when the U.S. government needs to send its proposals for changes to Europe for the 2016 Wassenaar meeting. Indeed, the best use of industry's comments on the proposed rule may be to begin flagging a series of critical issues for the United States at early meetings related to Wassenaar before February, rather than trying to rush a final rule to completion. For that reason alone, the time spent in getting this rule right, not only for the United States but for other Wassenaar countries, is a worthwhile investment of time.

In the sections that follow, the Coalition lays out its key concerns with each part of the proposed rule. It then discusses the inconsistencies with Wassenaar and several countries' implementation of that agreement, as well as with data security requirements in other industries and the U.S. government's own information sharing and security initiatives. Next, it looks at the consequences of the proposed rule, which would have a dire impact on cybersecurity in the United States. Finally, it offers a number of preliminary proposals to begin to help BIS develop a framework that might accomplish its goals, while also protecting critical cybersecurity products and methods.

II. CONCERNS WITH PROPOSED CONTROLS

The Coalition has serious concerns with the ambiguous and overbroad language used in the proposed rule, which would capture not only cybersecurity products, but also basic software development techniques more generally.

A. Effective Control of “Intrusion Software”

Intrusion software would be effectively controlled by the proposed rule, despite the stated intent of BIS to the contrary. The FAQs released by BIS on intrusion and surveillance items emphasize that “intrusion software” is not itself controlled, so the transfer of exploit samples, proofs of concept, and other forms of malware are not controlled.⁴ But it is not possible to

⁴ See, e.g., FAQs #1, #2, #10, #19, and #24.

effectively share vulnerabilities and exploits for defensive purposes, or to use defensive “intrusion software,” without using control and delivery platforms and sharing the equipment, software, and/or technology behind them. While there is ostensibly no direct control of “intrusion software” itself, as a practical matter, the controls are broad enough to effectively control intrusion software by controlling items that generate, operate, deliver or communicate with it, and technology for the development, production or use of such items.

Vulnerability testing and patching is a good example of how the proposed rule would effectively control intrusion software. BIS states in FAQ #12 that vulnerability scanners, which find potential vulnerabilities in a system without actually exploiting them and extracting data, would not be captured. But this ignores the reality of the process of vulnerability research, which is not about just finding potential vulnerabilities or even sharing proofs of concept. When finding vulnerabilities and reporting them, the most valuable information to share with a vendor to help develop a patch is the information on how the vulnerability can be exploited and how the exploits work, including the technology used to develop them. This helps the vendor understand the root cause of the vulnerability and develop a more complete and long-lasting defense instead of just a “band aid” fix.⁵ Then, in FAQs #10 and #19, BIS recognizes that controlled “technology” may be transferred during the reporting of a vulnerability or exploit, highlighting that this process will indeed be subject to these highly restrictive controls. And in FAQ # 13, BIS recognizes that the tools used to test vulnerabilities (which find vulnerabilities and extract data to prove the vulnerability is real) would meet the technical description of items controlled under ECCN 4A005 and 4D004. If BIS were to control the information flow about exploits, as it has proposed in this rule, it would have profound effects on companies’ ability to produce successful defenses.

Similarly, third parties often make “exploits” to provide update services and manual patching for commonly-used software products produced by other companies. Such third party participation is necessary to supplement the features offered by the original provider, or where that original provider has gone out of business or has stopped supporting its code, as is often the case for critical infrastructure. Unlike auto-updaters that are part of the original software, these third parties use “exploits” to deliver updates and patches into vulnerable programs and systems.⁶

⁵ While an exploit on its own is not sufficient for defensive purposes, as understanding the root cause of the vulnerability is necessary to create an effective defense, for *offensive* purposes a single sample of malware may indeed be enough—especially considering that often general purpose tools, which would likely not be captured by this proposal, can be used to deliver and communicate with it. *See generally*, Section VI.D. Thus, while this attempted distinction in the proposed rule hurts defensive efforts, it likely does little to stop the export of malware for malicious use.

⁶ *See, e.g.*, Collin Mulliner et al., *PatchDroid: Scalable Third-Party Security Patches for Android Devices*, <https://www.mulliner.org/collin/publications/patchdroid.pdf> (describing “PatchDroid, a system to distribute and apply third-party security patches for Android” because many Androids contain “known security vulnerabilities [that] cannot be updated through normal mechanisms since they are not longer supported by the manufacturer and mobile operator”). Another example is the Xen hypervisor used by Amazon Web Services (“AWS”). While the Xen hypervisor is open source, AWS uses a customized version that is not public. Sometimes

They use these “exploits” to defeat the integrity of the original system, bypassing its protective measures, modifying its standard execution path, and providing external instructions. Even if the “exploits” themselves are not controlled, the related controls appear to squarely capture parts of these update and patching tools that deliver and communicate with the components that actually apply the patch.

BIS should recognize that any items that are captured by the definition of “intrusion software” will be effectively controlled by the proposed rule. Products need tools to deliver and communicate with them in order to be useful and marketable. Additionally, companies need to communicate in detail about vulnerability reports with vendors to create an effective patch. Therefore, control of these delivery, control, and communication mechanisms, as well as technology for their development, production and use, acts as an effective control on defensive products qualifying as “intrusion software,” as well as on sharing vulnerabilities and exploits.

B. Overbroad Definition of “Intrusion Software”

The effective control of all “intrusion software,” as well as related systems, software, and technology, would be particularly damaging given how broadly that term is defined, encompassing tools and products that are purely defensive. Below we discuss each aspect of the definition.

1. Software specially designed or modified to avoid detection by “monitoring tools” or to defeat “protective countermeasures” of a computer or network-capable device

This first part of the definition of “intrusion software” is ambiguous in numerous respects, in a way that makes its scope overbroad.

a) “Avoid detection” and “defeat”

The terms “avoid detection” and “defeat” are unclear. For example, in its FAQ #8, BIS states that auto-updaters are not controlled because, while they “may need to interact” with monitoring tools and protective countermeasures, they are not “defeating” or “subverting” the system. However, the line between merely “interacting” and “avoiding detection” or “defeating” is not clear. The reason for this “interaction” is so the monitoring tools and protective countermeasures allow the update to occur uninterrupted, which could reasonably be interpreted as “avoiding detection” or “defeating” such measures. The drafters seem to be contemplating a distinction in the proposed rule between permitted interactions that defeat existing monitoring and protections and those with the same effect that do not have permission. But they did not make such a distinction in the proposed language. Moreover, it would not even be clear whose

this version needs to be patched for security vulnerabilities, and AWS must push these patches across the globe at an urgent rate. These patches are made by AWS itself, not Xen—and they are delivered worldwide before the security vulnerability is made public. *See* Brandon Butler, *What happens inside Amazon when there’s a Xen vulnerability*, NETWORK WORLD (Mar. 3, 2015), <http://www.networkworld.com/article/2892313/cloud-computing/what-happens-inside-amazon-when-there-s-a-xen-vulnerability.html>.

permission would matter. The user? The network owner? The author of the software? There are legitimate software updates that occur without the permission or even the knowledge of the user or owner, and others that occur without the permission or even the knowledge of the author of the original software.⁷ This is a complex problem that the proposed rule has not taken into account.

b) “Monitoring tools”

The scope of the term “monitoring tools” is unclear, and guidance from BIS has raised the additional question of whether it intends to exclude all monitoring tools from the definition of “intrusion software.” For example, BIS states in its FAQs that “anti-virus software” is explicitly excluded from the definition of “intrusion software” because it is a “monitoring tool.”⁸ However, BIS does not make any such broader exclusion explicit, raising serious doubts about the scope of the proposed rule. Simply because “avoid[ing] detection by monitoring tools” is part of the “intrusion software” definition, it is not obvious that a “monitoring tool” cannot also be “intrusion software.” For example, antivirus software itself could be classified as “intrusion software” because it modifies the standard execution path of software to intercept and inspect data passing through the network to ensure that malicious actors are not exploiting the software. And it often has rootkit capabilities—it operates under the user interface and subverts part of the operating system so that when a program or user takes an action, it can intercept the action, inspect it, and, if necessary, modify the result with or without the user’s knowledge. BIS has labeled this “rootkit” capability presumptively offensive; however, these capabilities are necessary for antivirus software because they are the only means of getting inside a system at a deep enough level at which they can effectively monitor for and catch malicious traffic before it can infect the system.

Neither “monitoring tool” nor “antivirus software” is included among the explicit exceptions in the proposed rule.⁹ It is therefore not clear whether BIS meant in its FAQ #8 that *all* monitoring tools that are also intrusion software are excluded or whether antivirus software is somehow distinct. There are plenty of examples of products, in addition to antivirus software, that can be both “intrusion software” and a “monitoring tool”—including some that can be used for both benign and malicious purposes. Take keyloggers, which have traditionally been seen as malicious malware that records keystrokes to steal information. But keyloggers are certainly

⁷ See, e.g., *supra*, Section II.A (discussing third party updaters who provide updates and patches where companies have gone out of business or stopped supporting their code); and *infra*, Section II.B.2.c (discussing software innovation and development of third-party software to be used with other companies’ software products, both of which often require modifying the standard execution path of a program or process without the knowledge of the original designer).

⁸ See FAQ #8.

⁹ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28858 (May 20, 2015) (“Intrusion software” does not include any of the following: a. Hypervisors, debuggers, or Software Reverse Engineering (SRE) tools; b. Digital Rights Management (DRM) “software”; or c. “Software” designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.”).

“monitoring tools,” although BIS presumably would not want to exclude them from the definition of “intrusion software.” This is just an example of how difficult it will be to draw lines effectively in this industry.

Even “monitoring tools” with a traditionally nefarious reputation have legitimate uses, such as endpoint security products that allow companies to monitor their networks or particular employees.¹⁰ These products, just like malicious keyloggers, extract user data. Both are “monitoring tools,” but also come within the definition of “intrusion software” (and often even have “rootkit” capabilities¹¹). The key difference is the intent of the customer and the authorization of the system administrator.

These examples show the importance of clearly defining “monitoring tools” and explicitly stating under what circumstances a product would be excluded from the definition of “intrusion software” where it may fit the definition of both (and could even have malicious uses).

c) “Protective Countermeasures”

The term “protective countermeasures” suffers from the same lack of clarity as “monitoring tools.” First, the uncertainty over whether there is an exception for “monitoring tools” raises the question of whether “protective countermeasures” are also excluded. Second, the language of the proposed rule does not make any distinction between defeating the “protective countermeasures” of *legitimate* systems and defeating the “protective countermeasures” that protect *malware*. Because of this shortcoming, a product aimed at defeating the protective countermeasures of malware, in order to defeat the malware, would fall within the scope of the rule.

Third, despite the short definition provided in the proposed rule, it is not clear what a “protective countermeasure” must protect in order to qualify as one. While the examples in the proposed rules emphasize Data Execution Prevention (“DEP”), Address Space Layout Randomization (“ASLR”) and sandboxing, which ensure the safe execution of code to protect the system and user, Digital Rights Management (“DRM”) software also often allows for the “safe execution of code,” but it does not protect the interests of the user; it protects the intellectual property of a third party. Would DRM be considered a protective countermeasure? Would defeating DRM software or “jailbreaking” a phone be considered defeating “protective countermeasures”? BIS seems to accept that it would be in FAQ #26, but without a detailed definition, the scope of “protective countermeasures” remains uncertain.

¹⁰ See, e.g. Bodi, Pilixo, <https://www.pilixo.com/resources/lp/computer-monitoring>; Computer & Mobile Monitoring Software, Webwatcher, <http://www.webwatcher.com/pc-monitoring>.

¹¹ For example, as can be seen in the websites in footnote 10, these “monitoring tools” are advertised for their “undetectable” and “tamper proof” methods, including hiding their processes from the monitored users and any antivirus software they may install.

d) “Network-capable device”

By including mobile devices and smart meters in the definition of “network-capable device,” BIS would introduce potential liability for mobile device users and other consumers that have no control over products that may be embedded without their knowledge. For example, if the rule is interpreted to cover both sides of a “communication” with malware (both the “controller” side used by the attacker and the “receiver” side on the hacked device), the owner of a phone that has been hacked and contains malware may violate the rule by taking the phone abroad without a license. While such an unwitting victim would not have had any intent to violate the controls, the EAR impose strict liability.

2. Performing any of the following: (a) Extraction of data or information, from a computer or network-capable device, or the modification of system or user data or (b) modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions

The second part of the definition of “intrusion software”—the requirement that it extract or modify data or modify the standard execution path of a program—captures a wide swath of legitimate programs.

BIS’s attempts to limit the definition leave many open questions. For example, in FAQ #11, BIS states that “[o]ther types of malware, including software that only leaves evidence of a successful security breach without further compromising or controlling the system” are not included. However, it is difficult to see how a program can leave evidence of a security breach without modifying the standard execution path of the program, executing externally provided instruction, and possibly modifying some data. Creating evidence of a security breach is not within the normal scope of software operation (normal working systems do not have a built in button that says “click here to show a breach”). The program “leaves evidence” of such breaches by changing the behavior of the system (modifying the standard execution path) and typically also modifying data to leave the trace (the equivalent of a note, “I was here.”).

While the concept of extracting or modifying data may be understandable, though very broad, there is no attempt to define “standard execution path of a program or process” and the potential breadth of what “modifies” such a path may capture a wide array of products. BIS has clarified that this language is meant to refer to a variety of techniques used to hijack, or otherwise corrupt, a legitimate (or otherwise trusted) application or process running on a computer, mobile phone, or other device.¹² It continues that this can be done for persistence or for other purposes, and that through these modifications, a remote operator (or remote command and control software) can execute commands or perform other tasks that further compromise or exploit the hacked (penetrated) device.¹³ However, there are problems even with this attempted clarification, which appears to define modifying a standard execution path as doing anything with a program or process that the original author did not intend. Again, without saying so, the essence of these controls appears to boil down to a question of intent. But if intent is what BIS meant, the definition needs to be more specific. A reasonable person could interpret “standard”

¹² See FAQ #30.

¹³ See FAQ #30.

to simply mean “default” or the path used the majority of the time. And if “intent” is what is necessary, the definition needs to be clear about whose intent matters (for example, it could be the network owner, the system user, the system administrator, or the developer of the software; and do these persons need to have predicted the exact modification that occurs, or is it enough that they intended some path modifications to occur?). Additionally, as discussed elsewhere in these comments, often legitimate computer programs change existing software—for the better—in a way that the original author did not intend or predict.

a) *No distinction between interfering with legitimate systems and processes and malicious ones*

Whereas FAQ #30 emphasizes hijacking or corrupting *legitimate* and *trusted* applications or processes, the language in the proposed rule itself does not make any distinction between hijacking and corrupting legitimate applications versus malicious ones.¹⁴ As written, the proposed language would apply to software meant to extract or modify the data of *malware* or to modify the standard execution path of *malicious* programs and processes (i.e. to defeat them).

For example, the rule would appear to capture malware recovery tools, which are used to regain control of a system infected by malware. When a user has lost control of its system to malware, the malware does not simply have an off switch to uninstall it. Instead, the malware will often put protective countermeasures in place to stop a user from uninstalling it, leading to a need for defensive tools that use exploitation (i.e. “intrusion software”). And such tools must be generated, operated, delivered, and communicated with in order to run effectively on the compromised system and defeat the malware.

A well-known example of such a protective tool is CISCO’s Talos TeslaCrypt Decryptor.¹⁵ This “decryptor” was developed to deal with a particular type of ransomware (a “cryptolocker”) that works by taking a system user’s valuable files (targeting photos, videos and documents) and encrypting them, after which a user has to pay a “ransom” to get them back. As a defense against this ransomware, CISCO released an “exploit,” its decryption tool, as well as the tools to run and deliver it. The tool works by defeating the protective countermeasures of the infected system to get at the malware, as well as the protective countermeasures of the malware itself; it then both (1) modifies the standard execution path of the malware to provide external instructions to interrupt and regain control of the system and (2) extracts data from the malware (to obtain the encryption keys) and from the infected system (to recover the encrypted files). In order to be practically used by average users, it has to be delivered to the computer together with

¹⁴ Additionally, even if the rule did explicitly make a distinction between “legitimate” and “non-legitimate” uses, this would be very difficult, if not impossible to determine in a technical sense. It would seem as though it would need to be based on someone’s approval (whether the network owner, system administrator, or authorized user of the software), but even this definition could run into problems if the approvals and knowledge of these actors conflict.

¹⁵ See Andrea Allievi, Earl Carter & Emmanuel Tacheau, *Threat Spotlight: TeslaCrypt – Decrypt it Yourself*, CISCO BLOGS (Apr. 27, 2015), <http://blogs.cisco.com/security/talos/teslacrypt>.

the tools to operate and communicate with it. As such, it would fall squarely within the definition of “intrusion software” and ECCN 4D004.¹⁶

This class of “exploits” and “intrusion software” has the explicit purpose of protecting users from other malware. Other legitimate tools—rootkit and virus uninstallers, adware removal suites, and ransomware remediation—act similarly to recognize, interrupt, and stop malware, and may be similarly covered.

b) Legitimate reasons to extract and modify data from or alter a standard execution path of a trusted system or process

There are legitimate defensive reasons to extract and modify data from or alter the standard execution path of trusted systems and processes. For example, the products of Ionic Security Inc. (“Ionic”) add additional security to legitimate programs, which the original program’s author did not contemplate and may not know about. Ionic’s products protect individual pieces of data, including those entered into cloud or desktop applications, so the data remains protected wherever it goes and to whomever it goes. It also allows the document owner to alter the access to their data remotely and retain control over access even after the data has left their physical control—a method of security that is of increasing importance with growing cloud computing and other trends. But, the products appear to be caught under the definition of “intrusion software” (and thus the controlling ECCNs as well). To secure this data, these products must alter the standard execution path of legitimate programs in ways that allow for the execution of externally provided instructions; and they must have equipment and software which operate, deliver, and communicate with them.

For example, to protect data entered into a network, Ionic uses a plug-in, through which data can be encrypted as it is entered.¹⁷ Unencrypted data never leaves the network, and the controlling keys to unencrypt the data remain with its creator. To do this, the plug-in must interrupt the flow of data; in essence, it diverts control of the program as the user sends data to use Ionic’s logic instead of the program’s standard path. This process requires the plug-in to interrupt the standard execution path of the program on which the data was created or stored, and extract and modify the data entered by the user, thus meeting both parts of this element of the

¹⁶ These malware recovery tools are also discussed briefly below for their ability to “communicate” with the ransomware, another reason they would be covered by ECCNs 4A005 and 4D004.

¹⁷ Currently, Ionic’s “plug-ins” for network content protection work with built-in plug-in architectures. In these situations, the original developer contemplated and intended plug-ins to be used to make changes or additions to the program. While these “intended” changes may not have been meant to be caught by the proposed rule, as discussed above, this is not entirely clear in the current language. For example, a reasonable interpretation of “standard” could be the “default” path, which plug-ins alter, even if alternative “execution paths” were contemplated in its original design. If “standard” was meant to convey a distinction of intent or authorization, such a distinction should be more clear; also, it would need to be specified whose intent or authorization is necessary (the original program designer? the user of the computer? the system administrator? the network owner? all of the above?).

definition of “intrusion software.” The plug-in receives a configuration that allows it to behave differently depending on the website being accessed, since different websites will require different methods to control and protect data. This also modifies the standard execution path of the websites in order to allow the execution of externally provided instructions regarding the protected data. To work effectively, such programs must also avoid monitoring programs, in order to provide a seamless interface and not set off antivirus software—thus meeting all elements of the proposed rule’s “intrusion software” definition.

A similar functionality of Ionic’s products can provide protection for individual pieces of data in a document, which the creator can set to different levels of access (public data, restricted data, etc.). To do this, the product makes modifications to the document and word processing software through a plug-in;¹⁸ the plug-in inserts itself into the software and interrupts the software’s processes. For example, to allow the user to save the document with Ionic’s encryption protections, the Ionic plug-in must interrupt the standard software program’s “save” workflow and instead instructs the system to use Ionic’s workflow. This involves hooking into the software’s standard code and modifying it to change how the document is saved, so that the document can be secured. And it is not necessarily done with the permission of the original software developer. This capability—to divert the behavior of the program to act differently than how it was meant to work (diverting the flow of the program to use the Ionic product’s code instead of its own)—seems to clearly qualify as modifying the standard execution path of a program, as well as extracting and modifying data; and it is again done to avoid setting off protective countermeasures or monitoring programs. Such program manipulation is necessary to make the security feature user-friendly and effective. And both its use (which requires tools to deliver, operate, and communicate with it—which include capabilities that Ionic needs to “export” to foreign customers) and development will be controlled under the proposed rule.

Various other functions of Ionic’s products also appear to be captured in the “intrusion software” definition. For example, in addition to providing encryption which follows individual pieces of data and allowing for remote changes to the data’s access controls, Ionic allows users to keep track of how and where their data is accessed, even once it has left their network. The plug-in extracts data from the system every time access to a protected item is requested to allow the policy services to decide if the data access should be granted. Such extraction of data again appears to fall within the definition of “intrusion software.”

Yet another example are the products Ionic offers to assist highly regulated industries with their compliance responsibilities. For example, some regulated industries, such as the financial services industry, are required to store their electronic communications for possible audits. However, due to web applications, such as Facebook and LinkedIn, businesses face compliance problems where their employees use such web applications to communicate in a way that is not recorded or logged. Ionic has worked to create an innovative solution to block certain features of these web applications (such as the messaging and posting features) on authorized

¹⁸ Unlike the network plug-ins discussed above, Ionic’s plug-ins that work with desktop software often work outside and go further than the software’s built-in “plug-in” architecture (if any exists) intended. In these cases, Ionic alters the “standard” execution path, however it is defined, in a way that was not intended or contemplated by the original developer.

devices to prevent such unlogged communications and help companies comply with their regulatory obligations. However, such products modify the standard execution path of software while the user is visiting controlled sites in order to allow for externally provided instructions. Specifically, Ionic provides an installer to introduce the Ionic software, and the Ionic.com platform communicates with the Ionic software to deliver policy rules for each site. As such, they, too, appear to be covered under the proposed rule.

Each of these products appears to come squarely within the scope of the controls, even though they are purely defensive and protective in nature. Even if they are classified as “intrusion software,” which is not itself directly controlled, as a practical matter they cannot be used without equipment and software that operates, delivers, and communicates with them, or developed without the “technology” used to develop them.

The proposed rule would not only capture Ionic’s products. It could capture many add-ons for software that do not come with a plug-in architecture or functionality, because add-ons work by modifying the standard execution path of the software to provide for externally provided instructions in ways the original designer did not intend.¹⁹ For example, the Microsoft Detours library is a key industry tool for software innovation, performance monitoring, and security patching. It is designed to generate “hooks” that intercept and modify the standard execution path of a target program and then generate instructions to deliver these execution changes into the program. It also captures a variety of tools that extract or modify data for legitimate reasons. For example, remote management software allows system administrators and information technology (“IT”) help desks to control computers remotely and often to extract information, such as to collect activity reports, from these computers to resolve any issues.

c) May encompass all software innovation

The broad and undefined phrase “modifying a standard execution path of a program or process” has the potential to encompass all software innovation. Such innovation often involves building on other people’s software, including defeating the protective countermeasures of the original developer or the system their software is running on, modifying the standard execution path that the original author wrote, and experimenting with how the software runs. As such, “modification of the standard execution path of a program or process in order to allow for externally provided instructions” could include many legitimate and innovative software engineering practices.

The proposed language similarly would appear to capture all third-party software developers—i.e. developers creating software to integrate with other companies’ products.

¹⁹ As discussed in footnotes 17 and 18 it is ambiguous whether the proposed language would also capture the numerous add-ons for browsers and other programs which do have an add-on architecture (i.e. add-ons that *were intended by the original software designer*). Such add-ons could be considered to alter a “standard” or “default” execution path, even though the original author intended the modifications to be made. This ambiguity highlights the importance of defining “modification of the standard execution path of a program or process.”

These developers create software to cure a flaw in or add new functionality to an existing program, which the existing program's authors did not originally intend. To add this functionality seamlessly, the new program by necessity takes steps that intrude on the old program, defeat any relevant countermeasures, and implement the new program's instructions to modify the "standard execution path." For example, performance monitoring tools are used by developers to improve their software and by system owners to understand why their systems are running slowly. They work by hooking into the system in different places to time how long certain processes take. To do this, they must defeat the system's protective measures to inject the hook, and then modify the standard execution path of the program in order to record the times for each process. Similarly, automation tools are used to automate the actions of a system user in order to test that a system is working properly. Such tools, when working with older programs that did not intend such automation, must inject hooks (in a way that defeats protective countermeasures) to change the standard execution path to allow simulation of the user's actions. This process is simply how new functionality is developed and added.

C. Exceptions to the Definition of Intrusion Software

The proposed rule's explicit exceptions to the definition of "intrusion software"—such as hypervisors, debuggers, software reverse engineering ("SRE") tools, and digital rights management ("DRM") tools²⁰—are inadequate and ambiguous. As an initial matter, considering the items described above, these exceptions are insufficient even for existing tools; and this approach (simply adding exceptions for legitimate products) is altogether ineffective because even if each and every legitimate product currently available was listed, it is not possible to predict which tools may be invented in the future.

Additionally, it is not entirely clear how these exceptions apply to products that can be used for both an "excepted" purpose (like DRM), but also have malicious uses. For example:

- Packers: These tools take "intrusion software" and put them into a format that is compressed using a unique algorithm, protected, and delivered to a target. If such a file contains malware, it will avoid setting off an antivirus product's alert unless that antivirus software knows its algorithm or runs it in a "sandbox" type environment. Such a tool, used in this way, seems to be the type of product BIS is trying to control—it delivers exploits. However, the same tools are also used in legitimate activities, such as for DRM purposes. In that context, the "packer" similarly takes information and compresses it into a format that is more difficult to analyze, but it does so in order to protect data from unauthorized access. Although this DRM purpose is explicitly excluded under the current proposed rule, it is unclear how BIS intends to differentiate between such products—they are technically indistinguishable, with only a different end-use. Again, the controls come down to intent.
- Obfuscators: These products are used to protect intellectual property by protecting its code from analysis. However, malware can also be run through such a tool to protect its code from analysis (making it harder for defenders to understand how it works and defeat

²⁰ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28858 (May 20, 2015).

it). These products work the same way and are, technically speaking, often the same. However, some are marketed for the protection of intellectual property and for other legitimate uses; while others are marketed for the protection of malware. It is, again, difficult to see how BIS intends to differentiate between such products or determine when they are designed for intrusion software versus other legitimate uses.

Under the proposed rule, it is not clear how BIS intends to handle these types of products, which may have both “excepted” uses and malicious uses. It seems difficult, if not impossible, to distinguish between them at a technical level; and if BIS intends to use an intent-based approach, it should do so explicitly.

D. Controlled Items Related to “Intrusion Software”

1. Systems, Equipment, Components, and Software (ECCNs 4A005 and 4D004)²¹

The proposed ECCNs 4A005 and 4D004—for systems, equipment, and components, as well as software, that is “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”—are too broad to be workable. As discussed above in Section II.A, the proposed controls effectively capture any “intrusion software,” including legitimate security tools, because these tools cannot be used without generating, operating, delivering or communicating with them. Even beyond that, as BIS has recognized, the language of the ECCNs themselves catch some legitimate defensive tools, such as for penetration testing, because they are themselves command and delivery platforms for “intrusion software.”²² These ECCNs would catch innumerable other purely defensive products, in addition to penetration testing tools.

a) Network Penetration Testing Products

As recognized by BIS, certain network penetration testing products will be captured by the proposed controls.²³ This result is inevitable because, like so many cybersecurity defensive and testing measures, the only difference between penetration testing and malicious hacking is the intent of the person using the tool. Companies who want to extensively test their systems need to go further than using basic penetration testers, which often only capture common vulnerabilities. These companies hire security professionals to access and test their systems using many of the tools and tactics that an adversary would use. Without using these same tools, there is no way to test that a system is secure against them. In other words, anything that controls the tools will make legitimate security penetration testing much more difficult, and these advanced penetration tests are critical to the security of companies and their products.

²¹ Existing ECCN 4D001.a, as it relates to “intrusion software,” is also of concern to the extent it controls software “specially designed” or modified for the development or production of the products described herein.

²² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015); FAQs #18, #29.

²³ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015); FAQs #18, #29.

For example, Symantec Corporation (“Symantec”) engages in extensive and rigorous internal product penetration testing for every new product that it sells to make sure it is safe for its customers. The testers use various systems (including hardware and software) to conduct the testing, and, during the testing process, write their own code to find vulnerabilities and exploit them. They then write a report containing all of the technical information they obtained in the testing process, including on vulnerabilities and exploits. This report is shared with the necessary people in Symantec, so the remediation to close those vulnerabilities can be swiftly developed and implemented.²⁴ This entire process involves Symantec’s labs both inside and outside the United States, and can also involve third parties who may or may not be in the United States. Most, if not all, major cybersecurity companies and information technology manufacturers use this type of penetration testing to ensure the safety of their products and networks.

This type of penetration testing is a normal security procedure on the customer side in addition to the supplier side. Such extensive testing of IT systems and networks is commonplace in many industries, including the nuclear power industry, electricity generation and distribution, financial services, and health care. Moreover, those customers often only buy software products to put on their networks and systems if the sellers can certify that the products are safe, including having been put through extensive penetration testing. The proposed rule’s controls on such penetration testing products and processes would severely hamper the current processes these industries and their suppliers go through to ensure their systems and products are safe.

b) *Other Tools*

There are various other purely defensive tools that may also be covered by the new ECCNs 4A005 and 4D004.

First, sandboxes for malware analysis. These tools use hypervisors to contain malware, and communicate through hypervisors to observe and communicate with malware. Considering the broad scope of the term “communicate,” these sandboxes, which are designed to communicate with malware in order to analyze it and monitor its processes, are potentially caught. Additionally, these sandboxes must have parts that take the malware they find on systems or networks and “deliver” it into the hypervisor in order for this analysis to occur. While hypervisors themselves are excluded from the definition of “intrusion software,” programs that “deliver” malware to hypervisors, “house” the “intrusion software” and ensure it is isolated, and then “communicate” with it are not so clearly excluded.²⁵ Similar products include:

²⁴ Additionally, if during this process Symantec learns of a vulnerability in someone else’s system, it shares that information with the company involved, which may also happen to be outside the United States.

²⁵ While sandboxes are explicitly included in the definition of “protective measures,” it is not clear whether they would also be (1) “intrusion software” itself, or (2) items under 4A005 or 4D004 that “communicate” with intrusion software. *See* Section II.B.1 (discussing how monitoring tools and protective countermeasures can also be intrusion software and expressing uncertainty as to whether the proposed controls would apply to such products).

- FireEye’s detonation chamber technology. This technology is present in many FireEye, Inc. (“FireEye”) products and allows users to execute suspicious email attachments, binaries and web objects, mobile applications and malware that may be resident in file content and malware stores against a range of browsers, plug-ins, applications, and operating environments that track vulnerability exploitation, memory corruption, and other malicious actions in a secure virtual environment. If an attack is identified, FireEye technology captures call back channels, dynamically creates blocking rules to protect the malicious code from infecting the system and transmits this information back to the FireEye network. In order to accomplish this, FireEye technology must communicate with intrusion software, extract data from a computer or network-capable device and modify the standard execution path of a program or process. This behavior seemingly falls squarely within the plain language of the proposed ECCNs.
- Emulators and other virtualization projects. These products re-implement the services that a computer provides (i.e. a symbolic execution) in order to emulate a program. They then capture malware, let the malware interact with the emulator, and monitor all instructions executed. They are important tools for defensive analysts to understand malware, especially as malware attacks on companies rise. Companies that provide such full system emulation approaches include LastLine²⁶ and BlueCoat.²⁷ Such items are necessary not just to run the malware, but to communicate with it and observe it to help security professionals obtain a deeper understanding of it and its threat indicators.²⁸ This communication with malware, even though it is for purely defensive purposes, would again appear to be covered by 4A005 and 4D004.
- Honey pots. “Honey pots” are “fake” computers that are purposely set up as virtual machines or simply software pretending to be a computer. The goal is to have malware infect these “computers” so defenders can observe it. However, once these “honey pots” become infected, they must communicate with the malware, and allow the malware to communicate back. Under the language of the proposed ECCNs, these purely defensive products appear to be covered and controlled.

Second, this language could capture rescue tools for systems that have already been compromised by malware. These recovery tools are used to regain control of an infected system after it has been infected by malware—for example, a “cryptolocker,” which encrypts all of the users’ files for a ransom. As discussed above in Section II.B.2.a, these rescue tools could themselves be classified as “intrusion software”; but even more simply, because they must

²⁶ Lastline Data Breach Platform, Lastline, <https://www.lastline.com/platform/security-breach-detection>.

²⁷ Malware Analysis Appliance, Blue Coat, <https://www.bluecoat.com/products/malware-analysis-appliance>.

²⁸ These products raise the question of whether “communicate” with malware means just pushing and pulling data back and forth (for attackers, this means command and control data, which sends instructions on what to do and the exfiltration of data from systems without the user’s or administrator’s knowledge), or whether it also includes hooking into malware and/or the system it runs in to monitor and analyze its execution.

“communicate” with the malware in various ways (including altering its execution path to interrupt it and regain control of the system, as well as extract data from it, such as the encryption keys to recover the stolen files), these tools appear to fall directly under proposed ECCNs 4A005 and 4D004.

Third, Automated Exploit Generation (“AEG”) tools automate the process of finding vulnerabilities by generating exploits.²⁹ These products can be used for offensive, as well as purely defensive, purposes. AEG is critical to defensive efforts because of the innumerable vulnerabilities in software. Companies must be able to quickly and efficiently determine which of these vulnerabilities are actually a threat (including some way to rank them). For example, if a vulnerability cannot be weaponized (i.e. standard protective measures are able to defeat it), it is not as big of a concern. AEG tools seek to generate “intrusion software” to test which vulnerabilities are of high or low severity. This process allows researchers to pinpoint for vendors the most dangerous threats and provide them with the deeper understanding of these vulnerabilities that is necessary for them to create a true defense. If such products are controlled, as they appear to be under the proposed ECCNs (because their entire purpose is to generate exploits), the rule would control the tools and research that is the most relevant and valuable to companies trying to protect themselves.

Additionally, encoders are tools that can be used to deliver “intrusion software” to a system, but also have legitimate uses not related to “intrusion software.” Such encoders can be used by malicious actors to deliver “intrusion software” because they take shell code, and put it in a format that can be delivered to a target without interference from protective countermeasures by masking any characters that would have been denied by such measures. However, the same class of tools, such as Base64 encoders, are also commonly used in emails and attachments to ensure that binary data is kept intact when stored and transferred over media that is designed to deal with textual data.

Finally, Return Oriented Programming Compilers (“ROPC”) help generate software that can be used in an exploit technique called Return Oriented Programming (“ROP”) to help test defenses against these ROP exploit techniques. This is not the standard way of generating code, and so could be considered to be designed to generate these ROP exploit codes. Such compilers generate ROP code, which overcomes data execution prevention (“DEP”) and may therefore be seen as designed to defeat protective measures. Thus, these compilers could be considered designed for the generation of “intrusion software,” even when used for defensive testing or research purposes.

2. Technology required for the development of intrusion software (ECCN 4E001.c)

The proposed rule adds new ECCN 4E001.c for technology required for the development of intrusion software. This control is very broad, with far-reaching consequences for the cybersecurity community, which depends on rapid and detailed information sharing across the

²⁹ For example, ForAllSecure, Inc. is a start-up company that provides automatic software to test for bugs in programs, including determining the bugs’ exploitability and prioritizing the bugs by their exploitability. *See generally*, ForAllSecure, Inc., *Mayhem: Software Testing Made Easy*, <http://forallsecure.com/mayhem.html>.

globe. As an initial matter, this proposed ECCN would control any technology for the development of cybersecurity tools that may be classified as “intrusion software,” such as those discussed above in Section II.B. But discourse, innovation, and experimentation are critical to developing new cybersecurity tools. These controls would severely damage global cybersecurity companies’ (such as Symantec’s and FireEye’s) ability to engage with their research and development teams abroad, which often closely collaborate with their U.S. teams in developing their cybersecurity products.

This proposed ECCN would severely restrict cybersecurity research and defense more broadly, including research and reporting of vulnerabilities and threat intelligence sharing. These effects seem to be recognized to some degree by BIS already, as the preamble to the proposed rule states that the technology that is proposed to be controlled includes “proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.”³⁰ But BIS does not appear to have recognized the effect these controls on such “proprietary research” would have on global security companies.

While this section focuses on ECCN 4E001.c, the same concerns apply to 4E001.a, “technology” for the “development,” “production,” or “use” of equipment or software controlled by 4A or 4D. ECCN 4E001.a would inevitably control technology (including technical discussions) for the development, production, and use of the purely defensive items that interact with “intrusion software,” such as those discussed above in Section II.D.1.

a) *Vulnerability Assessments and Testing*

Security vendor research groups and security companies, such as FireEye, work with “proprietary research” on vulnerabilities and exploitation every day in their labs across the globe when they conduct vulnerability assessments and testing. In fact, FireEye has a zero-day focus group that conducts this type of proprietary research and reports its results to vendors on a regular basis. When these companies find vulnerabilities, they need to report them and develop a defense as soon as possible. To do so, they need to share not only the vulnerability and exploit, but the information on how the exploits work, including the technology to develop them. To secure systems, defenses need to be developed within days of identifying vulnerabilities, staying as close to real-time as possible; such security gaps cannot wait weeks or months for a fix. The customer expectation is “as fast as possible” and the company that is faster at creating and sharing fixes and other intelligence has the competitive advantage. In the past year, FireEye has itself seen that entire cycle (from finding a vulnerability, understanding its exploitability, developing a patch and deploying it) take as little as 24 hours. But they are global companies and not all of their researchers are in the United States; this work is not even always completely internal to the companies. For example, many U.S. cybersecurity companies have official and unofficial sharing agreements, including for information regarding malware, all over the world

³⁰ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28854; see also FAQs #10 and #19 (recognizing associated “technology” that is controlled may be transferred with the reporting of a vulnerability and exploit); see also FAQs #24 and #25.

with security groups such as other countries' Community Emergency Response Teams ("CERTs").

Cutting U.S. companies off from interacting with these international groups will result in a dramatic decrease in the scope of U.S. security companies' (like FireEye's) knowledge into the global threat landscape, reducing their understanding of which types of malware are being used by malicious actors. Without this type of broad and up-to-date knowledge (and in this industry, knowledge needs to be updated on a daily or even hourly basis), U.S. companies' ability to contribute to the collective defense and protect their customers, including major U.S. companies, the U.S. government, and entities connected to U.S. critical infrastructure, would be greatly damaged. Particularly considering the policy of "presumptive denial" for items that incorporate "zero-days," this proposed rule could cause large numbers of zero-days that companies such as FireEye report responsibly to security vendors every year to go unreported because such reports necessarily include controlled information such as how the exploits work and the technology used to develop them. But it would do little to stop their continued use by malicious actors. The result would be a serious loss for the security community as a whole. And the foreign partners of these companies may also stop providing similar information to U.S. companies.

Similarly, though providing vulnerability testing services through a different model, companies like Synack, Inc. ("Synack"), who work with a talented global community of independent researchers, will also be severely affected by these controls on "technology." Synack recruits a network of researchers that spans thirty-six countries and combines their knowledge and expertise to conduct extensive vulnerability assessments for its customers, often global companies whose systems also span internationally. Through Synack's secure platform hosted in the United States, these researchers access its customers' systems. They find and analyze vulnerabilities, including by writing code to develop exploits to test the vulnerabilities' exploitability; then, they provide Synack with a vulnerability report that includes information on the vulnerability, how it was discovered, and how it was exploited, as well as information regarding their assessment of the severity and impact of the vulnerability on the customer's business. This information often incorporates information on "zero-days," since most of the vulnerabilities are previously unknown and do not yet have a fix. Synack's operations team validates the information and provides it to its customers. Each step in this process may involve foreign nationals—including the researchers, the Synack operations team, and the customers—either within or outside of the United States. The information that is shared inevitably includes in-depth technical information for the development of intrusion software (including how the vulnerabilities are exploitable and how the exploits work). This process would be inconceivable if Synack was required to obtain a license to communicate about each vulnerability report it receives or shares with its researchers and customers in various countries, especially considering that the company could potential face presumptive denials where such reports involve information on zero-day exploit capabilities.

b) *The difficulties in determining the scope of the "technology" will inevitably chill discourse among researchers.*

It is not clear how technical or specific a discussion would have to be before it would be considered controlled "technology," a level of uncertainty that would be sure to chill important

activity in this area. The definition of “technology” would encompass discussions between researchers about vulnerabilities and the means of exploiting them if they are sufficiently technical (i.e. they allow for the operation or building of intrusion software or a related item that is controlled). But these are discussions that inevitably occur both in the process of reporting a vulnerability and in developing a defense for it, as well as developing and innovating cybersecurity tools more generally.

BIS’s attempts so far to clarify the scope of the technology controls are not encouraging. In FAQ #4, BIS attempts to clarify what types of information would be and would not be controlled as technology for the development of intrusion software; however, the examples seem inconsistent with the definition of “intrusion software” and related controls. For example, BIS states in FAQ #4 that fuzzing, “trying different inputs,” and analyzing execution, including decompiling and/or disassembling code and duping memory, are not covered. However, these are common ways to generate zero-day exploits. It is unclear why BIS would state that these techniques for developing exploits, which would likely be controlled under ECCN 4D004, would not qualify as controlled development technology. “Fuzzing” provides invalid, unexpected, or random data to the inputs of a computer and then monitors the computer for crashes. The crashes caused by the “fuzzing” are then analyzed to determine if they involve a vulnerability that is exploitable. That is the purpose of fuzzing—to provide the information that is “required for” the development of the exploit. The first one to determine if such a crash is in fact exploitable, by reaching and exploiting it, discovers and generates a “zero-day” vulnerability.³¹ Without this full analysis, the vendor cannot know whether a crash has been caused by a non-exploitable bug or represents a true security vulnerability. BIS muddies the picture about which forms of technology are controlled by stating without any apparent reason that these particular methods (and the resulting information), which would appear to fall squarely within ECCN 4E001, are not controlled.

The difficulties in determining what is included under the proposed technology controls³² will have a disproportionate impact on the many small companies and independent researchers

³¹ Microsoft’s !exploitable (pronounced “bang exploitable”) is an example of such a program. This product is a Windows debugging extension that provides automated crash analysis and security risk assessment. It works by first determining the uniqueness of a crash and then assigns an exploitability rating for the crash.

³² In FAQ #4, BIS states that the only technology that would be controlled is that which is “required for” and peculiarly responsible for achieving or exceeding the relevant characteristics of controlled items related to “intrusion software.” But “peculiarly responsible” is difficult to interpret and apply. First of all, that concept is not currently defined in the EAR, although it is used in the definitions of “specially designed” and “required.” Its use in the definition of “specially designed” makes it integral to the definition of “intrusion software,” and the fact that it is part of the definition of “required” means it must be considered in any evaluation of the applicability of technology controls. Even without the ambiguities around the meaning of “peculiarly responsible,” the “specially designed” analysis is quite complicated. BIS has set out a definition for “peculiarly responsible” in the proposed rule that was published on June 3, 2015 that may provide some clarity. *See Revisions to Definition in the Export Administration Regulations*, 80 Fed. Reg. 31505, 31517 (June 3, 2015). But until that rule takes effect this term

who are not as well versed in export controls and who may be shut out of the market, or forced underground, because they do not have the resources to be able to comply with these complex and ambiguous rules. These rules were developed for major industrial and defense companies and do not work well in a market whose foundation is independent researchers and small companies with little overhead.

These ambiguities create an extraordinary grey area with the potential to chill innovation and discourse. If researchers are prevented or discouraged from engaging in covered communications, even within their own companies, the reporting of vulnerabilities and the ability to produce defenses effectively and quickly may be significantly affected.³³

E. Controlled “Surveillance” Items (ECCN 5A001.j)

The proposed rule adds ECCN 5A001.j for IP network communications surveillance systems, equipment, and components.³⁴ While this ECCN involves many elements that work to limit its applicability, concerns still exist with its language, which, similar to the “intrusion software” items, lacks a distinction between defensive and offensive items and could include tools companies use on their own networks to monitor activity and find hackers, as these tools look closely at the data that is moving through the companies’ networks in order to help keep it secure.

1. ECCN 5A001.j could capture tools used to help keep networks secure

For example, this definition could capture any of FireEye’s network appliances (such as FireEye endpoint and network forensic and investigative tools) because these products intercept network traffic, reassemble it, inspect and analyze it, and block or modify it when necessary. While likely not being the type of system that BIS intended to capture, these products come very close to the definition in ECCN 5A001.j as it currently stands, and, as demonstrated below, will only continue to resemble it more with time.

For example, network security monitoring tools, such as those available from FireEye, meet all of the elements in 5A001.j.1: they conduct analysis at the application layer, extract selected metadata and application content (including attachments, etc.), and index the extracted

remains undefined. In any event, the scope of BIS’s technology controls will remain beyond the capacity of many small companies and independent actors in this industry to analyze and comply with.

³³ Context is particularly important here. Many independent researchers are only now getting comfortable with responsibly reporting vulnerabilities to companies without the fear that the company will take legal action against them for accessing their systems. Enacting regulations with the types of ambiguities in this proposed rule would unnecessarily create fear of export enforcement action from the government for such reporting, and consequently reverse this critical progress.

³⁴ Relatedly, existing ECCNs 5D001 and 5E001 will control the software and technology related to these IP network surveillance systems. As discussed above, the breadth of these controls, particularly those around “technology,” are particularly concerning in the cybersecurity realm where detailed communication and collaboration is essential.

data (to inspect it, and modify or block it when necessary). They also have “hard selectors” passing through their system, such as email address and recipient information when processing email. Additionally, they meet element 5A001.j.2.a because they use email addresses, such as when an email address is known to be used by a bad actor (e.g. in a spam campaign), as “selectors” to be searched and targeted so an alert is triggered when emails from that address pass through the network. Finally, as to 5A001.j.2.b, their ability to “map relational networks” is only increasing. Such capability is desirable in a security monitoring system because it enables the system to correlate information and track two important groups: (1) the group of people being targeted or affected by the malware or attack, and (2) the group of attackers.

Similarly, this ECCN could cover email malware virtualization tools that help to secure and protect email, such as FireEye’s Email Security (EX Series). Such tools extract content from emails, including determining whether there are .zip file attachments and, if needed, look through human readable content to extract passwords for such files. They may also extract .pdf attachments, which are often used by malicious actors to deliver exploits to unsuspecting targets. These tools monitor email and extract human content to scan for malware and quarantine it before it can affect the target system. Such security tools, if of a “carrier class,” could come within the definition of IP network communications surveillance systems despite being completely defensive.³⁵

2. “Carrier Class” is not sufficiently defined.

Additionally, the proposed rule does not define “carrier class” to the degree necessary to enable companies to determine if their products are covered. BIS has attempted to narrow the scope of ECCN 5A001.j in its FAQ #14 to clarify that “carrier class IP network” was meant to capture systems at a national level IP backbone, such as those that handle data from an entire city or country. However, BIS also states that “carrier class IP network” was not defined because it was difficult to put precise parameters on the concept. Thus, no definable metrics (such as gigabytes per second, which is often used to measure network size) are associated with this “carrier class” parameter.³⁶ There are many different sized “cities” and “countries” and this

³⁵ Depending on how broadly the rule is interpreted, it could even cover items used by many companies, including Symantec and its customers, to make sure that their products (which are sold and downloadable online) are not sold to individuals from sanctioned countries. These items track and block IP addresses, so that individuals from these sanctioned countries cannot purchase online products. To do so, they monitor the network for IP addresses from sanctioned countries, pull out these IPs, and act on this information by blocking these users’ access to their website. These tools place tracking script on the companies’ websites in order to extract data and track the movement of users throughout the websites, and then feed this information into a system which can be searched for selectors, such as IP addresses. These tools are ubiquitous throughout the industry and are the only way to ensure that individuals from these sanctioned countries do not access online products. If there is any ambiguity whether these products would be covered, it could necessitate licenses for thousands of products.

³⁶ Even if BIS did put a certain “bandwidth” number on the scale, it would quickly be outdated—five years from now the bandwidth for a city may be commonplace for a house. Similar to how the definition of “supercomputer” fifteen years ago is no longer significantly different from a

metric seems entirely inadequate to help companies determine where their products fall.³⁷ For example, it is entirely possible that the DOD network is itself bigger than most cities' networks.³⁸ Also, there are large universities that are bigger than small cities. Would this mean the tools used to monitor and inspect the traffic in and out of these networks would be covered by this rule? While BIS may have meant to exclude most security monitoring products (including FireEye's products discussed above) with the "carrier class" limitation, this scale needs to be more clearly defined. If BIS cannot itself determine a clear place to draw the line, it is difficult to see how it can expect companies to be able to determine if their products are covered.

Additionally, it is unclear how the line would be drawn for "components" for "carrier class" IP network communications surveillance systems. Often the difference between a "carrier class" network surveillance system and a smaller system is not a technical difference—the same components can be used for each. Often, more components (more computers, etc.) are used to bring the surveillance system from a small neighborhood to the level of a larger region. A "load balancer" is then used to spread the work among the different appliances—each "component" handles a certain amount of traffic, which is multiplied by the number of components to get the larger scale (this is called "horizontal scaling" and is core to the engineering systems for modern traffic rates). It is thus unclear whether components for "carrier class" IP network surveillance systems would include any components that can be used in such a larger system (which would seemingly then encompass all smaller systems using the same components).

F. Specially Designed

All of the proposed controls are limited by the term "specially designed." But that term of art, defined in Part 772 of the EAR, can be difficult to apply in practice, particularly for smaller companies and independent operators that make up much of the U.S. cybersecurity industry. Moreover, the definition of "specially designed" does not seem to account for the

common desktop, such use of "bandwidth" as a metric, even if it seems ridiculously large today, in the future will not be.

³⁷ For example, North Korea has only 1,024 official Internet protocol addresses, fewer than many city blocks in New York. The United States, by comparison, has billions of addresses. Nicole Perlroth and David E. Sanger, *North Korea Loses Its Link to the Internet*, NY TIMES (Dec. 22, 2014), http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=1. Similarly, some estimates have put the bandwidth of North Korea's nationwide optical network at 2.5 Gbps. See *Asia Internet History*, available at: <https://sites.google.com/site/internethistoryasia/country-region-information/north-korea-korea-democratic-peoples-republic-of>. By comparison, Comcast has begun offering 2 Gbps fiber-to-home service in some areas; and already offers 10 Gbps fiber service to businesses. See Jon Brodtkin, *Comcast doubles Google Fiber with 2 Gbps symmetrical fiber service*, ARS TECHNICA (Apr. 2, 2015), available at: <http://arstechnica.com/information-technology/2015/04/comcast-doubles-google-fiber-with-2gbps-symmetrical-fiber-service/>.

³⁸ See, e.g., *JIE: How DOD is building a bigger network that's also a smaller target*, DEFENSESYSTEMS (Feb. 23, 2015), <http://defensesystems.com/Articles/2015/02/23/Joint-Information-Environment-JRSS-security.aspx?Page=4> (describing upgrades to the DOD network backbone that will increase the bandwidth to 100 Gbps).

realities of the information technology industry. For example, one key reason for finding that an item is not “specially designed” is that it was developed as general purpose, i.e. without knowledge that it would be used in or with a particular commodity or type of commodity.³⁹ But the note to that release paragraph says that in order for it to apply, there must be contemporaneous development documents that, in their totality, establish the necessary elements; absent such documents, the commodity may not be excluded from being treated as “specially designed.”

This provision does not account for the realities of the technology industry for several reasons. First, there often are no “documents” or any records at all showing the intent of a developer. Software developers often work alone and independently of any organization, so there would be no reason for them to document their design intent. Second, developers often experiment in a variety of ways, not always knowing exactly what they will uncover or create. In other words, they often do not set out on a particular mission that can be retrospectively traced to determine what their intent was in developing a particular product. That absence of a development intent trail would make it impossible to invoke this important exception to the “specially designed” concept for items that can be used for multiple purposes, such as the packers and obfuscators, discussed above in Section II.C. This is just one small example of how the existing structure of the EAR was not made to accommodate controls on such a unique, dynamic and complex industry. Attempting to squeeze a square peg into a round hole in this instance would have profoundly negative consequences.

G. “Publicly Available” and Intent to Publish

The EAR contain carve-outs for items that are “publicly available” or intended to be published. In its FAQ #5 on intrusion and surveillance items, BIS explains that the EAR does not control the export of data to conference organizers with the intent that it will be published at a conference. See also FAQ #6, which states in response to the question whether the regulations will make it more difficult to alert the world of exploitable bugs, that there are no restraints on publishing information otherwise subject to control. While it is generally positive to spell out clear exceptions in such a way, this particular provision raises serious concerns for the cybersecurity industry, because zero-day exploits and their associated technology often are not made publicly available until there is a defense available and released. The “responsible disclosure” process is as follows: a vulnerability is found, reported to the system or software vendor and discussed to determine impact and priority, then a defense may be developed and delivered to the vulnerable system, and after that a company may decide to publish the vulnerability. Companies often do not want a vulnerability or exploit to be published before a defense is released. For critical infrastructure systems in particular, for which the timeline for patching vulnerabilities is very slow, taking as long as twenty years in some cases, encouraging the publication of exploits before a fix is available may be unacceptably dangerous.⁴⁰

³⁹ Paragraph (b)(5) of the definition of “specially designed.”

⁴⁰ See, e.g., Kelly Jackson Higgins, *The SCADA Patch Problem*, INFORMATIONWEEK, DARKREADING (Jan. 15, 2013), available at: <http://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979?> (noting that only about 10-20% of utilities and other organizations running industrial control systems install patches that vendors release,

On the other hand, failure to allow the prompt exchange of technology and information related to the vulnerability would also be dangerous, as it would stall the process for developing a fix. In this way, the proposed rule constitutes a threat from both sides to the cybersecurity industry. It is not clear whether there is an acceptable solution within the confines of the EAR as they stand today, but it is clear that trying to fit this dynamic industry into the pre-set mold of outdated export control regulations will present real complexities that need to be examined closely before any final regulatory action.

Furthermore, many cybersecurity conferences may fall into a grey area in the rules. Typically these conferences include many nationalities but portions of the event may not qualify for the carve-outs that apply to those that are “open” or “public.” For example, the primary revenue stream for many such conferences involves private training offered by the speakers (either before or after the conference) that goes into more technical detail than could be covered during the conference. Additionally, some sessions may not allow all technically qualified individuals to attend, for instance by excluding members of the press or government.⁴¹ Because they may not qualify for the relevant carve-outs, in order to avoid the constraints imposed by the proposed rule, such conferences would in all likelihood be offered outside the United States in the future in order to facilitate attendance by foreign researchers, students and professionals. This would be just another way in which the center of gravity for this critical industry may move offshore, with potentially serious long-term consequences for U.S. national security.

III. LICENSING POLICIES

Due to the broad and ambiguous controls discussed above, the strict licensing regime proposed by BIS for cybersecurity items is alarming. The following sections discuss the Coalition’s key concerns regarding the proposed rule’s licensing policy, the effects of including deemed exports and intracompany transfers within this strict regime, and the burden of the proposed licensing application process on a cybersecurity industry that is constantly evolving and dependent on rapid sharing of information.

A. Strict Requirement for Licenses to All Destinations, Except Canada

The requirement for licenses to all destinations except Canada for cybersecurity items is unduly restrictive.⁴² Adding to the concern is the ineligibility of controlled items for any license exceptions, except certain provisions of License Exception GOV (exports to or on behalf of the U.S. government).⁴³ The rule also explicitly removes cybersecurity items’ eligibility for License Exceptions ENC, STA, and TSR. These unusually strict proposed licensing policies do not take

because of the complexity involved in avoiding system interruptions during the installation process).

⁴¹ Cf. 15 C.F.R. § 734.7 (information is “published” when it is released at an “open conference,” which means that, among other factors, all technically qualified members of the public are eligible to attend).

⁴² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28857-58 (to be codified at 15 C.F.R. § 742.6).

⁴³ *Id.* at 28856-57 (to be codified at 15 C.F.R. § 740.2(a)(19)).

into account the realities of the cybersecurity industry and are more stringent than the existing licensing policies for virtually all other items controlled under the EAR. The very existence of a licensing requirement in this industry would hinder U.S. cybersecurity activity and forestall the development of new capabilities.

The reality of the cybersecurity business is that vulnerabilities would be exploited by malicious actors while defensive products would become obsolete waiting for licensing approval. In the penetration testing context, BIS licensing would be completely unworkable. Penetration testers do not know what vulnerabilities they will find when they begin the testing; they follow any leads they discover and write code as they go to develop the exploits to test the vulnerabilities they find. And when penetration testers find something, they cannot just share the proof-of-concept exploit with the company that hired them (or in some cases the company did not hire them—they are freelancers). They need to share their in-depth technical knowledge on (a) the root cause of the vulnerability, (b) how they found it and generated an exploit against it, (c) their estimations of the ease of exploitation by malicious actors, and (d) proposed solutions to the problem, which (as the penetration testers did not develop the system being tested) requires in-depth technical discussions between the penetration testers and the company's engineering teams to suggest a workable solution (or 'patch').⁴⁴ It would be seemingly impossible to write a license application for such a project before it began, as the necessary information would not be known.

Furthermore, when a company engages in penetration testing it involves finding a company's most sensitive exploitable vulnerabilities (in order to develop patches for them). For this reason, the testing often takes place in a secure and isolated environment (a "black box"), with the information on the vulnerabilities and exploits protected while in the black box, and destroyed once the testing and patching is completed. If this information were to be leaked or otherwise released, the effects on the tested company and its customers could be crippling. If U.S. security companies that provide such testing services could be required to put this information into a license application, their customers would choose to use non-U.S. providers so to avoid what they may see as an unnecessary danger. For many companies, including Symantec, this penetration testing process involves collaboration with individuals outside the United States as well as foreign national employees within the United States, both of which would require licenses under the proposed rule. For example, Symantec's internal penetration testing process involves sharing information with its labs in Europe and India and also often involves third parties whom Symantec hires to test its systems. Also, if and when a company does face an actual breach of its systems, U.S. security companies have "incident response" teams, who are ready to go at a moment's notice and sometimes have to deploy within 24 hours when a problem is discovered—these teams do not have time to get a license.

Additionally, the international cybersecurity community includes a significant number of independent researchers, many of whom have only informal relationships with U.S. cybersecurity companies. Many independent researchers are completely unaffiliated with any

⁴⁴ See also *supra*, Sections II.A and II.D.2.a (discussing the in-depth back-and-forth dialogue between independent researchers, security companies, and their customers during the processes for vulnerability testing and assessments).

security companies and can appear out of the blue when they choose to responsibly report vulnerabilities. Once a vulnerability is reported, however, companies need to engage in a back-and-forth dialogue with the researcher that would involve technology transfers to understand the vulnerability and its exploitability, and to develop a patch. These vulnerabilities (which if they are new and novel are by many definitions “zero-days”) need to be patched immediately. The entire cycle from finding the vulnerability, understanding its exploitability, developing a patch and deploying it can occur within 24 hours—there is no time to get a license. And even those independent researchers, who act as consultants and experts for companies who are trying to test their defenses and develop patches, often never sign a formal contract or arrangement. These independent actors, who are undoubtedly unfamiliar with the U.S. licensing process and may be reluctant to share their information with the U.S. government, will be discouraged from cooperating with U.S. cybersecurity companies and may choose to altogether withdraw from these informal engagements with U.S. companies if such licensing is required.

Even independent of the problems with applying a strict licensing scheme to the unique cybersecurity industry, the specific requirements for license applications for cybersecurity items would themselves be unduly burdensome. They incorporate the current reporting and registration requirements for encryption products, while eliminating eligibility for the encryption license exceptions. The proposed rule also adds new requirements specific to cybersecurity items that are very burdensome. For example, it would be difficult, if not impossible, for companies to explain how rootkit or zero-day exploit functionality would be precluded from the item. As described below in Section III.B.2, trying to identify how an item supports or precludes rootkit or zero-day exploit capabilities in the first place would be difficult and confusing both because they are undefined jargon terms and because they are often capabilities present in defensive products and research. In addition, determining the amount and type of information necessary to describe the “cybersecurity functions” would also be challenging. The requirement to share source code upon request could hamper the communications and collaboration that are key to building successful defenses by discouraging cooperation with independent software engineers. Those individuals would not stop working, but they would stop working with U.S. companies.

The number of license applications under this rule, for each new product, customer, foreign national employee and business partner, would not only tax the resources of the companies, but would swamp BIS as well.⁴⁵ For example, Symantec estimates that under the proposed rule (in addition to the hundreds of deemed export licenses it would need) it would need several hundred hardware, software, and technology licenses for its products, as well as a couple of dozen of site licenses. Licenses would be required not only for cybersecurity

⁴⁵ It is difficult to estimate the number of cybersecurity companies in the United States that would be affected by this proposed rule, but it is likely in the thousands. Due to the low overhead in this industry, businesses can often be started without external help or capital, making venture capital firms unnecessary. In any event, it is clear that it is an industry that is growing rapidly. *See* Rick Gordon, *The Cyber Security Market Is Hot! Here’s Why*, INFORMATIONWEEK, DARKREADING (May 8, 2014), <http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128> (“A dozen years ago the \$3.5 billion security market was dominated by five vendors. Last year, VCs bankrolled 230 startups.”).

companies and researchers but also for their customers. These customers often have individuals (such as in their IT departments), who may be foreign nationals or located in foreign offices and coordinate with the cybersecurity companies to conduct penetration testing or use other defensive tools that may be covered by the proposed rule. The range of companies requiring licenses could include financial institutions, pharmaceutical companies, and other companies in highly regulated areas that must use penetration testing and other covered security products.⁴⁶ And the range and number of companies that choose to (or are legally required to) conduct such testing is growing. In short, requiring companies to obtain licenses for the export of these types of systems, software, and technology would be devastating to the U.S. cybersecurity industry, and—just as importantly—would be a blow to cybersecurity itself.

B. Explicit Licensing Policies for Certain Items

If licenses are required, the licensing policy framework as currently envisioned is at odds with efforts by U.S. companies to implement strong cybersecurity mechanisms. While the proposed rule does state a favorable licensing policy for some items, and a presumptive denial for others, these policies are nowhere near sufficient to assuage concerns and in some instances seem to make little sense. And, outside of these explicit policies BIS has given companies little guidance on what to expect from the licensing process, instead proposing a case-by-case licensing policy to determine if a transaction would be contrary to U.S. national security or foreign policy interests.

1. Favorable Licensing Policy

BIS's favorable licensing policy is not nearly sufficient. It is limited to certain countries based on type of end user: (1) U.S. companies or subsidiaries, but only those located outside Country Group D:1 (includes countries like China, Russia, and Vietnam) or E:1 (Cuba, Iran, North Korea, Sudan, and Syria); (2) "commercial partners" in Country Group A:5 (includes many European countries, plus Australia, Japan, South Korea and Argentina, among others); and (3) government end users in Australia, Canada, New Zealand, and the United Kingdom. There are many important countries that are excluded from this list. For government end users, even most European allies are excluded. And for U.S. companies and subsidiaries, some of the excluded countries are those in which it is most important for U.S. companies to use cybersecurity defenses to ensure their networks are secure, such as China and Russia.

Even if one of these favorable policies does apply, considering the pace at which products are developed and new versions updated (including updates required for continued integration with third party products), companies could be required to repeatedly apply for licenses and would face damaging gaps in their products' ability to integrate with third party products—a result likely to overwhelm both their own resources and those of BIS. And the

⁴⁶ See, e.g., Federal Information Security Management Act (FISMA) of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3544(b)(5); see also *Technical Guide to Information Security Testing and Assessment*, U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-115 (September 2008); *Penetration Test Guidance*, Federal Risk and Authorization Management Program (FedRAMP), Version 1.0.1 (July 6, 2015). See generally, Section V, below.

complexity, risk and processing time for licenses would chill activity in this industry that operates in real-time. For example, in the vulnerability research context, if a vulnerability is discovered, a company is likely to have teams around the world working on a fix in real time. If the vulnerability is made public, this process becomes a 24/7 race between the defenders and the malicious actors: the malicious actors use the public information about the exploit to develop exploit kits and exploit targets and the defenders rush to develop detections and mitigations and release these updated protections into their products globally. Requiring a license will stall this process for defenders, leading to less secure systems and causing customers to resort to security testing companies that are not subject to U.S. jurisdiction.

2. Policy of Presumptive Denial

The proposed rule includes a policy of presumptive denial for items that have or support “rootkit” or “zero-day” exploit capabilities. This policy is highly troubling in many ways. First, there are no definitions of “rootkit” or “zero-day” exploit capabilities, which are jargon terms that can be interpreted in various ways in different contexts. For example, zero-day exploits could refer to vulnerabilities that no one knows about except the attacker; but, they could also more broadly refer to vulnerabilities for which a patch is not yet available. But more importantly, a policy of denial would be devastating to the cybersecurity industry’s ability to develop and employ defensive products in light of the many critical and legitimate uses that exist for such items.

a) Zero-days

First, the policy of presumptive denial for items with zero-day capabilities would limit the development and delivery of defenses for the most dangerous vulnerabilities, zero-days. Zero-day vulnerabilities and their exploits make up the majority of what is discovered during penetration testing, as these are the previously unknown and unpatched vulnerabilities. In fact, as discussed above in Section II.D.2.a, companies such as FireEye have zero-day focus groups, which specifically research these types of vulnerabilities and must exchange information about their exploitability to develop a defense. If zero-days are defined as vulnerabilities without a released patch, then they are the highest priority items for responsible companies to address, and it would be highly problematic if they were restricted in their ability to get information about such vulnerabilities and associated exploits, technology, and technical details to—and from—their most knowledgeable experts, some of whom will be foreign nationals.⁴⁷ If a company was prevented from closing a vulnerability, the security of its customers would be at risk.

In FAQ #22, BIS explains that the reason for this policy of presumptive denial is that when a rootkit or zero-day capability is incorporated into a product or system, or if an exploit delivery tool is specially programmed to deliver or command this specialized malware, it is

⁴⁷ Relatedly, the patch that these experts develop and need to deploy internationally to close a zero-day vulnerability itself could be considered controlled under the proposed rule. The defensive products that contain the patch have in fact been used in the past by malicious actors to recreate the exploit. Because this ability exists in the very patch that is being exported to close a vulnerability, such a patch could itself be interpreted to be “technology” or “software” to develop or generate a zero-day.

presumed to be offensive by design. The intent appears to be to focus on denying malicious control and delivery platforms. However, that is not the practical effect. In fact, imposing such a harsh licensing policy on the export of tools with zero-day capabilities does not appear to accomplish what it sets out to do. Zero-days are zero-days because of the state of knowledge of others (i.e. they are not publicly known). Thus, this proposed policy would appear to control a delivery tool that carries a zero-day today, even though the exact same delivery tool might not incorporate a zero-day tomorrow (because the exploit has become public). This control makes it very difficult to pinpoint when delivery technology, which itself may stay exactly the same and can be independent of the exploit, is controlled. In other words, the “delivery tools” are often not unique for zero-day exploits; in some cases a generic delivery tool can be used.⁴⁸ The exploit is what is unique, and while the exploit and the delivery tool can be combined into the same tool (i.e. the same set of code), they also can remain distinct (i.e. two distinct sets of code). Delivery tools themselves can remain constant for the same “class” of target vulnerability while being updated with new zero-day exploits. This would appear to create a curious result—zero-day exploits would not themselves be controlled, and delivery tools without zero-days would not be subject to the policy of denial; thus, somebody could theoretically export them separately to be combined overseas, even though if they had been combined earlier any license would have been denied. This framework is clearly unworkable.

b) Rootkits

The presumptive denial for rootkits is similarly confusing. While the functionality of “rootkits” may vary and the term can mean different things in different contexts, a “rootkit” capability is often understood to mean simply that the item can live underneath the user interface and subvert what the user is doing without his or her knowledge. Basically, the rootkit subverts part of the operating system by interrupting it, running “underneath” it, or hooking into it; then, when the operator of the system takes an action, the “rootkit” intercepts that action and modifies or subverts it without the user’s knowledge so that it acts differently than it was intended to.

If this common definition is how BIS interprets “rootkit” capability in the proposed rule (which is unclear since no definition is provided), any software security instrumentation framework could be seen to create a rootkit capability. Security modules often hook into and change the behavior of the operating system. And a fundamental part of most security vendors’ endpoint protection products, including FireEye’s, is its “rootkit” capability. When you install antivirus software, FireEye’s endpoint security products, or various other types of security software, they often work by hooking into the normal operating system, monitoring the data communicated through it, intercepting and inspecting the data, and potentially changing it when it is a threat—all without user knowledge. These “rootkit” capabilities are used in these products

⁴⁸ Additionally, as discussed Section VI.D, the proposed rule is ineffective because it would likely not capture these generic delivery tools, as well as many other common and generic items that have legitimate purposes, but can also be used to deliver, operate, and communicate with malware, including zero-day exploits. See, e.g., Dennis Fisher, *Attackers Exploiting Windows Ole Zero Day Vulnerability*, THREATPOST (Oct. 22, 2014), <https://threatpost.com/attackers-exploiting-windows-ole-zero-day-vulnerability/108958>.

because they are the most effective means of getting into the system to monitor for and catch malicious traffic before it can get into the system.

“Rootkit” capabilities are a common function of legitimate software, not just for cybersecurity. Legitimate programs, such as DRM software, which the proposed rule exempts, could fall under a common understanding of the meaning of “rootkit” capabilities. Other examples include remote control software used by help desk technicians, system administration, technical support, and even anti-cheat mechanisms for video games. None of these programs with “rootkit capabilities” are intended to be malicious, but the proposed rule does not distinguish between those used with a network or system administrator’s or authorized user’s knowledge and authorization and those put there with only the malicious actor’s knowledge. In light of the broad range of legitimate uses for “rootkit” capabilities, a policy of presumptive denial would be inappropriate.

C. Deemed Exports

Applying the deemed export rule under such a strict licensing regime and without any license exceptions⁴⁹ would be devastating to U.S. cybersecurity. Even if BIS was able to craft some kind of blanket licensing authority for major companies, the many foreign nationals who work independently, such as academics and independent researchers, a significant portion of whom have only informal relationships with U.S. cybersecurity companies, would face serious restrictions that would also impact the major companies that rely on their expertise. Furthermore, this would affect companies using cybersecurity products, who would be driven to favor non-U.S. products in order to facilitate access by foreign nationals and overseas facilities.

1. U.S. Cybersecurity Companies’ Employees and Independent Researchers

U.S. cybersecurity companies employ many foreign national researchers, code writers, and others. For example, Symantec alone estimates that under the proposed rule it would be required to get up to 850 deemed export licenses. Given the very high number of foreign nationals employed in the cybersecurity field in the United States, this could mean tens of thousands of employees—or more—could be affected.

That does not even count foreign national independent operators living in the United States, many of whom only have informal relationships with U.S. companies.⁵⁰ Just as with the independent researchers in foreign countries discussed in Section III.A, these researchers often find and choose to responsibly report vulnerabilities to U.S. companies, which then need to engage in a back-and-forth dialogue with the researcher that would involve technology transfers to understand the vulnerability, its exploitability and severity, and to develop a patch. These researchers also act as consultants for U.S. cybersecurity companies when they have particularly useful expertise in a certain vulnerability or type of exploit. But the prospect of having to

⁴⁹ See FAQ #32.

⁵⁰ See, e.g., Acknowledgements, Security TechCenter, Microsoft, <https://technet.microsoft.com/library/security/dn820091.aspx> (listing individuals who disclosed vulnerabilities to Microsoft, including number of individuals who are unaffiliated with any organization and individuals identified only by an alias).

determine the nationality of independent researchers under the sometimes complex nationality rules BIS uses, and obtain the detailed personal information necessary to apply for licenses, is a non-starter. Many independent researchers would disengage from this process altogether at least with respect to U.S. companies, as they would view the drawbacks of this type of regulation as clearly outweighing any benefit they receive from responsible reporting. Such a scenario would be devastating for U.S. cybersecurity.

2. University Research

A large proportion of students and other researchers at U.S. universities in cybersecurity fields are foreign nationals.⁵¹ While publicly available information that arises during or results from “fundamental research” is not subject to the EAR, not all university research falls under this exclusion. For example, as is often the case when companies fund university research projects,⁵² any non-disclosure agreement or proprietary component would preclude publicly available treatment. If foreign nationals are not allowed to work on these projects, it will limit commercial funding of academic research, a key way that professors and graduate students are funded. These restrictions would severely impact not only U.S. cybersecurity, but academia and science and technology research more broadly.

3. U.S. Companies Outside of the Cybersecurity Industry

In addition, a broad range of U.S. companies that are consumers of cybersecurity technologies would face the burden of deemed export restrictions, many for the first time. The impact of this rule would be vast.

⁵¹ According to a 2013 report by the National Foundation for American Policy (“NFAP”), foreign students (who are not lawful U.S. permanent residents), make up 70.3% of full-time graduates in electrical engineering and 63.2% of full-time graduates in computer science. Stuart Anderson, NFAP, *The Importance of International Students to America* at 1-2 (July 2013), available at http://www.councilforglobalimmigration.org/ADV_NFAP_Report_July_2013 (“Foreign graduate students are crucial in assisting in research that attracts top faculty and strengthens the academic programs at U.S. schools, which benefits U.S. students and ensures America retains its preeminence as a teaching center in science, technology, engineering and math (STEM) fields.”).

⁵² For example, the University of Idaho, Center for Secure and Dependable Systems (“CSDS”) “works with companies and government agencies to analyze and design software that safeguards computer infrastructure.” Ysabel Bilbao, *Staying Well Ahead of Hackers and Protecting the Public*, CSDS, University of Idaho, <http://www.uidaho.edu/engr/csds/projects/staying-ahead-of-hackers>. See also Cybersecurity Research, Center for Cybersecurity, University of South Florida, <http://www.usf.edu/cybersecurity/research/> (“USF has a long and successful record of securing federal and industry funding. . . .”); Cybersecurity Research, Seidenberg School of Computer Science and Information Systems, Pace University, <http://www.pace.edu/seidenberg/cybersecurity/research> (“Skimmer Fraud Research funding has been provided by Association of Chartered Certified Accountants.”). Ionic is also currently planning collaboration on a research project with Dartmouth College, as well as sponsorship of a senior research project at Georgia Institute of Technology, University of Tulsa, University of Illinois Urbana-Champaign, or Dartmouth College.

D. Intracompany Transfers

The absence of a license exception for intra-company transfers or internal use⁵³ is highly problematic given the breadth of the restrictions. This may preclude multinational companies from purchasing U.S.-origin cybersecurity products, because of the globally integrated nature of their networks. The favorable licensing policy for certain intracompany transfers would not be enough to bring those customers back, both because of the very existence of a licensing requirement, and because it would not apply to countries such as Russia and China where cybersecurity needs are great. Companies prefer integrated solutions and would be very reluctant to use a provider whose product would be restricted in countries like China and Russia. While the intent of this policy is to prevent transfers of controlled technology to these countries, the effect would be the opposite, depriving U.S.-based companies of their best defenses where they are the most vulnerable. Often attackers only need to find the weakest link in a network to access its systems, so good protection in one country is of little value if it does not apply in another country. For this reason, customers may begin to prefer a non-U.S.-origin product that they can use enterprise-wide.

IV. THE PROPOSED RULE IS BROADER THAN WASSENAAR REQUIRES

In light of its impact on cybersecurity, it would be prudent for BIS, at a minimum, to restrict the proposed rule to the scope required by the Wassenaar Arrangement. However, there are areas in which the proposed rule appears to control a broader scope of cybersecurity items than other Wassenaar countries' analogous rules and imposes more stringent licensing requirements. For example, while Wassenaar and the European Union control lists use the same definition for "intrusion software" and the same categories for new items, the U.S. proposed rule arguably goes further by explicitly including network penetration testing products and proprietary research on vulnerabilities and exploitations, and stating a license policy of presumptive denial for items that have "rootkit" and "zero-day" exploit capabilities.

Additionally, as a practical matter, it appears the EU regulations have so far not been enforced as strictly as the U.S. proposed rule likely would be. For example, Hacking Team is an Italian firm that offers hacking tools and support to foreign governments, including tools that use malware. In the United States, licenses for such products would only be favorably viewed for a few countries. In the European Union, however, according to documents revealed in a recent hack of Hacking Team, the company was supporting sales of malware exploitation to numerous governments, including, but not limited to, Egypt, Ethiopia, Nigeria, Sudan, Malaysia, Bahrain, Vietnam, Saudi Arabia, Oman, and the UAE. And the company said in their leaked emails that their product is covered by Wassenaar, that it submitted license applications to the Italian government for sales to new customers (including a global authorization to allow export freely in all Wassenaar countries), and that it is in compliance with export control laws including the recently imposed Wassenaar protocols. Since it has continued its services, it has presumably obtained all of these licenses—an unlikely result under the U.S. proposed rule. The U.S. government should not impose the Wassenaar rule in a way that disadvantages its own companies.

⁵³ See FAQ #17.

A. Differences in the Applicability of the General Software Note and Mass Market Exception to Cybersecurity Items

A clear example of the United States applying stricter controls than the EU, Canada, and Australia is how the controls on “mass market” cybersecurity items will be implemented. In the United States, under the proposed rule, cybersecurity items are not eligible for either the “mass market” license exception or the lesser-controlled ECCN available for “mass market” encryption items (ECCNs 5A992, 5D992, and 5E992).⁵⁴ By contrast, under Wassenaar, and as implemented in the EU, Canada, and Australia, cybersecurity items without encryption appear to be eligible for exclusion under the General Software Note’s “mass market” provision, and, if they incorporate encryption they are still eligible for decontrol under the Cryptography Note (Category 5, Part 2, Note 3).⁵⁵

By including mass market items specifically excluded under Wassenaar and other countries’ implementing regulations, the U.S. proposed rule would require licenses for a broader scope of items than other Wassenaar countries. Such products could include Metasploit (Metasploit Pro), which is a penetration testing software that is openly sold in near retail fashion.⁵⁶

BIS’s rationale for this broad scope—that it is necessary for consistency with the existing treatment of encryption items⁵⁷—is not convincing. Cybersecurity items do not all have or need encryption capabilities, and the export of cybersecurity items, especially those without encryption, should not suffer from an overbroad attempt at “consistency.” Additionally, despite BIS’s assertions, the proposed rule does not treat encryption items and cybersecurity items consistently. It imposes heavier restrictions on all cybersecurity items (with or without encryption) than on encryption items themselves. At the very least, if cybersecurity items with encryption functionality are to be controlled consistently with existing encryption regulations, the “consistency” should extend to *both* the restrictions *and* their eligibility for license exceptions and less restricted ECCNs.

⁵⁴ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28857 (to be codified at 15 C.F.R. § 740.13(d)(2)); see also FAQs #23, #31.

⁵⁵ See *The Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List* at 3, 86 (March 25, 2015) (hereinafter “Wassenaar List”); see also Commission Delegated Regulation (EU) No. 1382/2014, 2014 O.J. (L 371) at 4, 141 (Oct. 22, 2014) (“hereinafter EU No. 1382/2014”); *A Guide to Canada’s Export Controls* at 1, 78 (Dec. 2013) (“hereinafter “Canada’s Guide”); *Australia, Defence and Strategic Goods List* at 62-63, 212-213 (April 8, 2015) (hereinafter “Australia’s List”).

⁵⁶ Other examples of mass market products are penetration testing software offered by Cobalt Strike (<http://www.advancedpentest.com/>) and Core Security (<http://www.coresecurity.com/core-impact-pro>), as well as similar tools that automatically generate and deliver exploits to verify vulnerabilities, such as Acuetix WVS (<http://www.coresecurity.com/core-impact-pro>) and NetSparkler (<https://www.netsparkler.com/web-vulnerability-scanner/false-positive-free-web-security-scan/>).

⁵⁷ See FAQs #23, #31.

B. Differences in the Applicability of the Exceptions in the General Technology Note to Cybersecurity Items

The General Technology Note is also implemented differently in the United States than in other Wassenaar countries. In the EU, Canada, and Australia, the General Technology Note, as under Wassenaar, provides that “[c]ontrols do not apply to that ‘technology’ which is the minimum necessary for the installation, operation, maintenance (checking) or repair of those items which are not controlled or whose export has been authorised.”⁵⁸ There does not appear to be a limitation in applying this provision to cybersecurity technology. In the United States, however, this General Technology Note provision is implemented through License Exception TSU,⁵⁹ which is not available for cybersecurity items.⁶⁰ BIS should not apply different treatment than other Wassenaar countries in this way.

V. INCONSISTENCIES WITH OTHER SECURITY COMPLIANCE REGIMES AND INFORMATION SHARING INITIATIVES

Additionally, the numerous federal data protection requirements and information sharing initiatives⁶¹ are in direct tension with the proposed rule, which restricts the ability of companies to use necessary tools for data and network protection and restricts the flow of information about cybersecurity tools.

A. Financial Industry

1. Gramm–Leach–Bliley (GLB) Act⁶²

For example, the GLB Act has numerous data protection requirements, which could be more complicated for companies to implement under the proposed rule. It requires “financial institutions”⁶³ to ensure the security and confidentiality of information they collect about

⁵⁸ Wassenaar List, General Technology Note, at 3; *see also* EU No. 1382/2014 at 4; Canada’s Guide at 1; Australia’s List at 62.

⁵⁹ *See* 15 C.F.R. Part 774, Supp. No. 2 (“License Exception TSU is available for “technology” that is the minimum necessary for the installation, operation, maintenance (checking), or repair of those products that are eligible for License Exceptions or that are exported under a license.”).

⁶⁰ *See Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28856-57 (to be codified at 15 C.F.R. § 740.2(a)(19)).

⁶¹ While these comments focus on relevant federal requirements, there are similar individual state requirements for data protection that may also be implicated by the proposed rule. For example, Massachusetts regulations impose security standards for the possession, licensing, storage and transmission of personal information about state residents that must, at a minimum, include reasonably up-to-date versions of system security agent software with malware protection and reasonably up-to-date patches and virus definitions, and the receipt of current security updates on a regular basis. Mass. 201 CMR 17.00, Section 17.04.

⁶² P.L. No. 106-102 (Nov. 12, 1999).

⁶³ This includes not just banks, but also insurance companies, financial advisers, nonbank lenders, loan brokers, tax preparers, providers of real estate settlement services, appraisers, courier services, ATM operators, credit reporting agencies, and debt collectors. The FTC is one

individual consumers, under the “Safeguards Rule.”⁶⁴ Specifically, it requires financial institutions to develop, implement and maintain “reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information”⁶⁵ and “a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.”⁶⁶ For large institutions, complying with these data requirements often involves extensive penetration testing that is in line with industry standards, but would be controlled under the proposed rule.

The GLB Act also requires financial institutions to “[d]esign and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.”⁶⁷ The risk assessment should cover “[i]nformation systems, including network and software design, as well as information processing, storage, transmission and disposal.”⁶⁸ It also instructs financial institutions to “[e]valuate and adjust your information security program in light of the results of the testing and monitoring.”⁶⁹ Again, to satisfy these requirements for “risk assessment” in line with industry standards, large institutions often engage in penetration testing that would be captured by the proposed rule.

The GLB Act also requires financial institutions to take steps to ensure that affiliates and service providers safeguard customer information as well.⁷⁰ FTC guidance⁷¹ suggests specific information security measures, many of which could be complicated by the proposed rule, including:

- Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;

of eight federal regulatory agencies that has the authority to enforce the financial privacy law, along with the state insurance authorities. The federal banking agencies, the Securities and Exchange Commission and the Commodity Futures Trading Commission have jurisdiction over banks, thrifts, credit unions, brokerage firms and commodity traders.

⁶⁴ This FTC rule applies to all businesses, regardless of size, over which the FTC has jurisdiction that are “significantly engaged” in providing financial products or services. *See* GLB Act §§ 501, 505(b)(2); 16 C.F.R. Part 314, 67 Fed. Reg. 36,493 (May 23, 2002).

⁶⁵ 16 C.F.R. § 314.1(a).

⁶⁶ *Id.* § 314.3(a).

⁶⁷ *Id.* § 314.4(c).

⁶⁸ *Id.* § 314.4(b)(2).

⁶⁹ *Id.* § 314.4(e).

⁷⁰ *Id.* §§ 314.2(b), 314.4(d).

⁷¹ *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, Federal Trade Commission (April 2006), available at: <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

- Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.
- Use an up-to-date intrusion detection system to alert you of attacks;
- Maintain up-to-date firewalls;
- Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- Use antivirus and antispymware software that updates automatically;
- Use a Secure Sockets Layer (SSL) or other secure connection when transmitting credit card information or other sensitive financial data to protect the information in transit; and
- Encrypt sensitive data if it must be transmitted by email.

The proposed rule would complicate companies' ability to comply with the GLB Act's mandate to use intrusion detection systems, monitor network activity, and test the security features of their network and software design and data storage and transmission procedures. Imposing export controls on products designed to operate, deliver or communicate with intrusion software would make it more complex for companies to use intrusion detection systems as required by the GLB Act, because as discussed throughout these comments these testing and defensive tools often must operate, deliver, or communicate with intrusion software. In particular, the proposed rule would complicate these companies' ability to conduct comprehensive testing on their networks, software and hardware, if they were restricted in their ability to use those systems across the entire company network (including facilities overseas) or to allow access by foreign national employees or service providers. Even if made workable by revisions to the proposed rule, imposing a BIS licensing requirement on top of an FTC information security obligation would present an undue burden for many small companies. Similarly, the proposed controls on IP surveillance systems may conflict with the GLB Act's requirement to monitor network traffic.

2. SEC and FINRA

Relatedly, Rule 30 of SEC Regulation S-P (referred to as the "Safeguard Rule")⁷² requires every broker, dealer, investment company and registered investment adviser to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information . . . reasonably designed to:

1. Insure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

⁷² 17 C.F.R. § 248.30(a), 65 Fed. Reg. 40,362 (June 29, 2000), amended by 69 Fed. Reg. 71,329 (Dec. 8, 2004).

The proposed rule would limit companies' access to the types of tools they need in order to comply with these mandates.

B. Payment Cards

The Payment Card Industry Data Security Standard ("PCI DSS") is a set of security standards to which major credit card companies have agreed to adhere and to enforce against merchants. The PCI DSS are applied against all organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any cardholder data, essentially any merchant that has a Merchant ID ("MID").⁷³ Under the newly released PCI DSS 3.0 and 3.1, any business that stores, processes or transmits payment cardholder data **will need to perform penetration testing** based on industry standards.⁷⁴ Such testing is required at least on an annual basis and after any significant change in the network infrastructure or applications. But the tools to do this testing may not be as accessible under the proposed rule because licenses will be required for multinational companies to use penetration testing tools from U.S. companies throughout their global networks.

C. HIPAA (HITECH)

Similarly, the Health Information Technology for Economic and Clinical Health ("HITECH") Act requires the protection of data in the electronic transmission of health information and strengthens the civil and criminal enforcement authorities of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in this area.

The HITECH Act provides for the creation of a National Coordinator for Health Information Technology within the Department of Health and Human Services and requires the holder of that office to include specific objectives, milestones and metrics with respect to: the incorporation of privacy and security protections for the electronic exchange of an individual's health information; and ensuring security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable.⁷⁵

The proposed rule, by restricting cybersecurity products, would make compliance with such requirements more difficult for multinational companies, who must provide these protections throughout their global networks.

⁷³ See generally PCI Security Standards Council, *available at*: <https://www.pcisecuritystandards.org/index.php>; see also *PCI FAQs*, PCIComplianceGuide, ControlScan, *available at*: <https://www.pcicomplianceguide.org/pci-faqs-2/#2>.

⁷⁴ See *Information Supplement: Penetration Testing Guidance*, PCI Security Standards Council (March 2015), *available at*: https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

⁷⁵ Pub. L. No. 111-5 (Feb. 17, 2009), Section 3001.

D. Other U.S. Export Control Requirements

The proposed rule is also inconsistent at a broad level with the recent proposed rules from BIS and DDTC⁷⁶ offering a safe harbor from export controls when information transmitted or stored abroad in electronic form is protected by adequate end-to-end encryption. While on the one hand recognizing the importance of strong security features like encryption to the successful operation of an international business, BIS has proposed new controls that would restrict access to and development of similar critical technologies. Some components of an end-to-end encryption solution, which BIS relies on for the effectiveness of its new safe harbor provision, would in some cases be subject to the intrusion software controls and thus would be less widely available and subject to innovation-stifling licensing requirements. For example, the Ionic products described above encrypt data wherever it goes and allow access restrictions to be set by location (such as to disallow access from outside the United States), so they may be among the products that would both be useful in implementing BIS's envisioned export safe harbor but also restricted under the proposed rule. Consistent with the approach BIS took in crafting the encryption safe harbor, the U.S. government should recognize the paramount importance of world-leading cybersecurity capabilities.

Similarly, License Exception TMP, 15 C.F.R. § 740.9, and other provisions of the EAR already require the protection of data. License Exception TMP requires that software used as a tool of trade be "protected against unauthorized access," including with secure connections, passwords and firewalls. Under License Exception TMP, the exporting, reexporting, or transferring party and the recipient of the technology must take security precautions to protect against unauthorized release of the technology. Such requirements are inconsistent with limiting access to the equipment, software, and technology that could provide such protection.

E. U.S. Government Information Sharing Initiatives

The proposed rule also conflicts with the priority placed on information sharing by both the Administration and Congress, for instance, the numerous information sharing programs developed by the Department of Homeland Security,⁷⁷ and those in the Intelligence Community.⁷⁸ The rule would severely restrict information sharing in the cybersecurity industry by imposing sweeping licensing requirements and restrictions on access to information by foreign nationals and by persons outside the United States. For instance, the Industry Consortium for Advancement of Security on the Internet ("ICASI") is a trusted private forum for internet companies to proactively collaborate to analyze, mitigate, and resolve multi-stakeholder,

⁷⁶ *Revisions to Definitions in the Export Administration Regulations*, 80 Fed. Reg. 31505, 31517 (June 3, 2015); *International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions*, 80 Fed. Reg. 31525, 31537 (June 3, 2015).

⁷⁷ See, e.g., U.S. Department of Homeland Security, Cybersecurity, Information Sharing, <http://www.dhs.gov/topic/cybersecurity-information-sharing>.

⁷⁸ See, e.g., *Strategic Intent for Information Sharing 2011-2015*, Office of the Director of National Intelligence, available at: <http://www.dni.gov/files/documents/Strategic%20Intent%20for%20Information%20Sharing.pdf>.

global security challenges. ICASI is not a fully open forum,⁷⁹ so the BIS rule may restrict its ability to operate effectively.

VI. CONSEQUENCES OF THE PROPOSED RULE

As discussed herein, the proposed rule would control defensive tools that companies use to keep their own software, networks, and infrastructure safe. Such broad controls of legitimate defensive products would negatively impact cybersecurity, chill research and innovation, and disadvantage the development of cybersecurity solutions in the United States. Information sharing and collaboration are the foundation of an effective cybersecurity industry. The proposed licensing policies would shatter that foundation and make continued research and development, and security operations, nearly impossible to conduct in the United States.

A. Companies' Ability to Protect Their Own Networks

The result of these broad controls would be to make it more difficult for cybersecurity companies to protect their customers and the general public from cyber-attacks. Restricting access to the cybersecurity tools discussed in these Comments could weaken the security of companies and their products, while doing little to stop the use of these tools. By prohibiting even the intracompany transfer of cybersecurity items, these rules complicate the use of such items for protective or testing purposes by U.S.-based multinational companies and their foreign subsidiaries. Additionally, due to the rule's overbroad restrictions and ambiguities, legitimate activities, such as threat intelligence sharing (which often discusses the technology and tactics of the adversary's intrusion software) and security research on attack techniques, may be regulated and discouraged. Such information sharing and research is essential to create better software and defense mechanisms. Harsh regulation could result in fewer vulnerabilities found and shared, fewer fixes and defenses made, and ultimately less secure systems. And if research and international collaboration are discouraged in the United States more than elsewhere, the United States' leadership and expertise in this field will atrophy, putting the United States at a distinct security disadvantage.

For example, the proposed rule would affect the ability of multinational companies to communicate and share information internally to develop protections. Companies have to go through many steps to develop defenses, including testing their systems for vulnerabilities, developing exploits to more fully understand and prioritize the vulnerabilities, sharing this information with vendors to collaborate in developing a defense to secure the system, and developing and using a system for efficiently delivering the defense into the existing product. The proposed rule appears to require licenses at every step. These extreme restrictions would halt companies' ability to go through the steps of fixing vulnerabilities.

Additionally, companies' research teams are finding these vulnerabilities and writing these exploits in real time. When a vulnerability is discovered, the process begins

⁷⁹ ICASI says on its website that it engages in "selective expansion of membership" and collaborates with "targeted industry groups and other bodies so that trust among members and participants is maintained." See *Our Mission & Goals*, ICASI, available at: <http://www.icasi.org/our-mission/>.

immediately—the idea of having to wait for a license is a non-starter. It is not even a matter of days, but minutes, usually just a few minutes. The company engages right away in a back-and-forth dialogue with outside experts, who may be non-U.S. persons and may not have (or ever form) a formal relationship with the company. Even if the company’s primary security provider is the beneficiary of some kind of blanket license, the third parties that the security provider may need to bring into the process likely would not be. This entire process of patching a vulnerability needs to be completed within days in order to prevent its exploitation by malicious actors. However, this entire process would be subject to licensing requirements under the proposed rule, which is clearly not workable no matter how liberal the licensing policies. Ultimately, these controls would leave companies and the public, both within and outside the United States, much more vulnerable to attack and unable to respond effectively.

B. Security Research and Innovation

Probably no other industry relies as heavily on daily, real-time innovation as the cybersecurity industry—it is constant and relentless. The breadth and ambiguity of the proposed rule would also have a profound chilling effect on the research and development of critical cybersecurity items.

Cybersecurity research teams, in companies and academia, work on a wide variety of projects that involve techniques that would be caught by the proposed rule. An example of the type of innovation that would be precluded in the future under the proposed rule is BlackIce, one of the early network defense technologies for Windows. BlackIce was not made by Microsoft, but worked by hooking into Windows, diverting and modifying its path of execution in order to provide its security functionality. It used an innovative technique that had not been used before. If the developers had been restricted by regulations similar to the proposed rule, it would have never been developed. As discussed above in Section II.B.2.c, almost all software innovation requires “modifying the standard execution path” of a program because it involves building on and improving other people’s software in ways they did not contemplate or intend when they wrote it. Therefore, the proposed rule would chill innovation across the entire software industry, not just in cybersecurity.

In the cybersecurity community, communication is key to innovation. If researchers in the United States cannot quickly and efficiently communicate with researchers in other countries, they would be cut off from this global community and would fall behind their peers. Such communication cannot be limited to merely providing samples as BIS has proposed—it must dive into the details of the technology that was required to find the vulnerability and generate the exploit. Even within companies, the proposed rule would seriously impede the ability to work and collaborate with colleagues abroad and foreign nationals in the United States on the development of more secure products and addressing current threats.

A clear example of this is sharing exploit toolkits, which are tightly controlled by malicious actors, who aim to prevent good actors from getting ahold of them and tailoring countermeasures for them. Exploit toolkits themselves allow bad actors to easily deliver exploits to a system, and upgrades and additional exploits can be added to a toolkit. These toolkits come ready and easy to use, with all of the tools to operate, deliver, and communicate with the exploits. There is an entire underground business which has been built around such toolkits to

aid exploitation. While it may be desirable to control malicious actors from using and sharing these toolkits, as a practical matter, the proposed rule will not stop sharing by malicious actors, who will continue to share these toolkits, including on the black market and outside the United States. What the proposed rule would do instead is prevent law-abiding security professionals from quickly and effectively providing defenses for such toolkits. As a practical matter, when a security professional manages to get ahold of such a rare toolkit, it is the practice to share it with other security companies with which there are formal or informal mutual sharing agreements (including internationally) in order for these companies to develop defenses. Because these toolkits include not just exploits but also the entire framework for delivering and communicating with them, they clearly fall into the regulated categories. But to create defenses, companies frequently need to share the entire toolkit (not only the exploits, but the tools in the kit used to operate, deliver, and communicate with the exploits) to learn how the toolkit hides, protects, and delivers its exploits. By preventing companies from sharing this information, the proposed rule would make it much more difficult for defensive companies to access these offensive tools in order to test and defend against them.

The effects the proposed rule would have on FireEye's threat intelligence sharing efforts are another example of its negative repercussions. FireEye anonymously exchanges data on email, web and file based threats on an hourly basis across its global customer base via its Distributed Threat Intelligence (DTI) cloud. This ensures that FireEye customers are protected against the most recent attacks FireEye has seen across its global customer base. This data may include technical indicators, contextual information, malware command and delivery tools, malware samples and other data that provides a clear picture of the malware infrastructure, capabilities and methodologies used by the attackers. The more extensive these descriptions of the exploit and the richer the pool of data, the better the defenses that FireEye is able to provide to its customers. If FireEye is unable to share this threat intelligence in near-real time across borders, FireEye customers, including many federal, state and local government customers, would not be protected from the most recent cyber-attacks. This situation would leave organizations unnecessarily vulnerable to exploitation.

FireEye also shares data with other companies and research labs to enhance the collective defense of the community at large. If this information were not able to cross borders, it would cripple this type of intercompany dialogue, as well as FireEye's and other U.S. companies' internal processes. If that were to occur, the United States would be left out of cutting-edge cybersecurity research and development.

C. Effectiveness of the U.S. Cybersecurity Industry

It is in the United States' security interests to have a strong and vibrant U.S. cybersecurity industry, so to have access to expertise and cutting edge defenses within its own shores. It should be an industry that the United States invests in and encourages. But the proposed rule would stymie the development of the cybersecurity industry in the United States, causing U.S. capabilities to lag behind those in countries with less onerous restrictions and ultimately come to depend on them for its cybersecurity needs. The proposed rule would act as a direct restraint on U.S. cybersecurity companies with a global presence, who use resellers, channel partners, and a network of sales and marketing agents around the world, not to mention their own foreign national employees and research partners and overseas facilities. But it would

also restrict cybersecurity companies' ability to sell their products even within the United States. Multinational companies want products they can use enterprise-wide, and putting a restriction on the use of U.S.-origin products may act as a complete barrier to contracts with these companies. Cybersecurity companies, which depend on rapid information-sharing to remain competitive, would be encouraged to minimize their presence in the United States.⁸⁰ In this way, the proposed rule would severely hamper the development of cybersecurity defenses in the United States, while driving that expertise to our strategic competitors.⁸¹

D. Ineffective in Controlling Malicious Intrusion Software and Surveillance Items

Although the proposed rule would be certain to damage the cybersecurity of the United States, it would not accomplish its goal of controlling the malicious use of intrusion software and surveillance items. First, unlike other highly regulated industries, the cybersecurity community does not operate in organized teams under a corporate parent. Malicious actors in this realm can act independently—all they need is a computer—and from anywhere in the world. Licensing requirements, while likely to stop or slow the law-abiding defenders, would have very little effect on the activities of malicious actors. Malicious tools will continue to be widely available on the black market or from China or other non-Wassenaar countries (and possibly even other Wassenaar countries like Russia), because “exporting” lines of code requires only seconds of access to the internet.

Additionally, the controls themselves, even if implemented seamlessly, would be ineffective in preventing the generation, operation or delivery of, or communication with, malware. The reason is simple: almost any software can be used for those purposes. As discussed above in Section III.B.2.a, generic delivery tools can be used to deliver malware into a system. Additionally, normal websites may be used for “Command and Control” (“C2”) for intrusion software, which includes operation, communication, and potentially delivery. For example, malware has used, without any modifications required, Google Docs, various email

⁸⁰ BIS should take care to not repeat the mistakes of the cryptography controls put in place in the 1990s, which were a major impediment to the development of security technology in the United States.

⁸¹ Many of these countries are already competitive in this realm, but the proposed rule would shift the competitive landscape very significantly in their favor. In China, where there is a growing market for such products, companies are increasingly investing in these areas. For example, Sempian Technologies, Ltd, a Chinese network solutions company with the slogan “cyber monitoring expert,” is starting to develop more sophisticated IP network surveillance equipment. The same is true in Israel. Examples include: ECI Telecom Ltd. (an Israeli company that delivers comprehensive networking to service providers); Hybrid Security (an Israeli cyber software vendor, whose Telepath product automatically learns typical user behavior patterns within web applications); Netline Communications Technologies (an Israeli company that specializes in communication jamming and detection systems and sells products including cell phone interception and RF monitoring); Votiro Inc. (an Israeli company that develops software packages to protect networks and IP infrastructures); White-Hat Ltd. (an Israeli penetration testing firm that does cyber defense consulting, 24/7 response, and penetration testing). All of these companies would benefit from decreased competition from U.S. companies and pushing cyber expertise outside of the United States.

services, and other legitimate websites and services for C2 purposes when trying to access a system. Though some malware may be made with specialized tools, most intrusion software is “generated” with tools that developers worldwide use every day (i.e. standard software development environments and coding languages). Using such standard tools for malware attacks is in fact advantageous for malicious actors because protective countermeasures cannot single out such tools as easily, so they tend to leave a smaller trace.

Even if there does exist a small number of U.S. companies both whose tools would be captured under the proposed rule and who sell these tools to bad actors, these companies can easily and immediately move underground or offshore, resulting in no real security benefit. And the U.S. government must ask itself if catching and denying one or two license applications from bad actors, who will continue to sell their products either by simply not applying for a license the second time around or by moving offshore, is really worth the drastic decrease in the United States’ cybersecurity abilities that it would cause and the resources for Commerce to issue the thousands of licenses it would necessitate.

The problems we have laid out above are only illustrative. The larger point here is that the proposed rule is unworkable and it will be virtually impossible to fix it within its current structure. Our hope is that the comments BIS receives in response to this proposed rule will make clear to the government what is already painfully apparent to industry—that it is extremely difficult to craft export control regulations in this sector that will account for its complexity and dynamism. The very existence of a licensing regime, even with broad and liberal license exceptions, would greatly discourage and hinder the U.S. cybersecurity sector. Because this export control licensing regime would also have very little effect on the transfer of malicious malware, it would be advisable to return to Wassenaar to attempt to draft a regulation that is better suited to accomplish its goals and better targeted to not capture legitimate cybersecurity efforts.

VII. PROPOSED SOLUTIONS

The fundamental framework of the proposed rule is critically flawed and cannot be fixed with a few simple changes. Below, the Coalition has laid out a few ideas that could be more effective in addressing the problem of malicious cyber activity, as well as some suggestions for ways the proposed rule may be made somewhat less harmful to industry. However, the Coalition feels the best option would be for the U.S. government to return to Wassenaar early next year to rework the 2013 agreement if it wants to correct the significant problems with this proposed rule.

The fundamental problem is the idea of imposing traditional export controls based on classification and destination on cybersecurity items. That approach will have a massively disproportionate impact on legitimate actors, far more so than in other industries. The cybersecurity sector is unique in part because bad actors operate almost entirely electronically, and are not easily subject to monitoring for compliance with a Commerce Department licensing requirement, and the good actors rely so heavily on speed, flexibility, international scope and information sharing that any licensing regime, no matter how it is structured, would stymie their effectiveness.

Moreover, U.S. companies are heavily dependent on the expertise of a mobile and global community of independent operators and losing access to them would mean that U.S. companies would be unable to stay on top of the threat environment. In this industry, the difference between being one step ahead and one step behind is everything. If our companies lose that critical edge, U.S. cybersecurity will be at risk. And the global community of independent operators—if they were made subject to a licensing requirement, or forced to share their data with the U.S. government—would simply opt out and drop back into the shadows. They are not like traditional manufacturers, for instance, who are part of the formal global economy, and therefore have to submit to whatever regulatory requirements are imposed on them. Instead, these individuals often make a living informally, and are more than capable of doing so. We hope that the U.S. government will take account of these important factors that make this industry unique, and craft a regulatory regime around this reality, rather than trying to shape the world to fit its rules, because this world is formless and cannot be squeezed into a box.

Finally, the U.S. government and the U.S. economy, along with the rest of the world, rely heavily on the U.S. cybersecurity industry, and they are expected to come to rely on it even more with time in order to stay secure and competitive in the digital age. We hope that policy makers will get serious about this issue while the door is still open, and redirect their efforts towards a productive path. Below we sketch out the contours of such a path.

A. Solutions That May Work

As described below, we believe that tinkering with the current proposed rule will not work. However, we will first briefly mention a few ideas for how the problem of malicious cyber activity may be addressed in a more effective way.

1. Criminal Law

One tool to counter malicious cyber activity, and the one with the least likelihood of having damaging side effects, would be the general criminal law.⁸² Rather than spinning its wheels on the currently proposed rule, the U.S. government should dedicate these resources to an existing capability that will work: the FBI and federal prosecutors. While the Commerce Department does have investigative capabilities, it has far less experience in the cyber realm than the FBI and Justice Department, and cannot bring the same kinds of tools, global resources and

⁸² An example of criminal prosecutions in this area include the recent international takedown of the Darkode forum, a marketplace to purchase and trade malware and hacking tools. This takedown involves arrests in 20 countries and indictments of 70 individuals, including 12 in the United States. Bill Chappell, *Malware and Hacking Forum Darkode is Shut Down; Dozens Arrested*, NPR (July 15, 2015), <http://www.npr.org/sections/thetwo-way/2015/07/15/423196810/malware-and-hacking-forum-darkode-is-shut-down-dozens-arrested>. Another example involves a Pakistani man who was indicted for conspiring to advertise and sell StealthGenie, a spyware application that could monitor calls, texts, videos, and other communications on mobile phones without detection. *Pakistani Man Indicted for Settling StealthGenie Spyware App*, Washington Field Office, Federal Bureau of Investigation (Sept. 29, 2014), <https://www.fbi.gov/washingtondc/press-releases/2014/pakistani-man-indicted-for-selling-stealthgenie-spyware-app>.

expertise to the table. BIS is skilled at regulating the noncompliant side of normal commerce. The FBI specializes in underground criminal activity. The problem with malicious cyber-attacks and intrusions of privacy does not stem from noncompliant or unethical U.S. companies—it is a problem that is based largely overseas and works with underground criminal networks and abusive foreign governments. Those are not threats that BIS is well-suited to address. To the extent there is a small portion of this threat that relies on U.S. companies, that portion would easily and immediately move offshore and this proposed rule would be worth no more than the paper it was written on as soon as it was issued (although its negative effects would persist).

2. Sanctions

In tandem with criminal law enforcement, the U.S. government can tackle this threat through trade sanctions, including so-called “secondary” sanctions that apply to non-U.S. persons. The Treasury Department’s Office of Foreign Assets Control (“OFAC”) is already engaged in this area. Executive Order 13,694 (April 1, 2015) provides for blocking all property and interests in property within U.S. jurisdiction of “persons” determined to have engaged in “cyber-enabled activities” occurring “in whole or in substantial part” outside the United States that may constitute a significant threat to the “national security, foreign policy, or economic health or financial stability of the United States” and that have the purpose or effect of:

- (A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- (C) causing a significant disruption to the availability of a computer or network of computers; or
- (D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.”

That order also separately covers activities involving “trade secrets misappropriated through cyber-enabled means.”

OFAC can play a significant role in supporting criminal law enforcement efforts by dedicating more resources to implementing this order. To-date, no designations have been made under Executive Order 13,694, so its deterrent effect has been limited.

3. Part 744.6 Controls

It may also be possible for BIS to play a productive part in this effort, but it cannot look anything like the role envisioned under the current proposed rule. We will set out a few ideas below with the goal of sparking a more productive conversation on this topic, but we have to preface this section by underscoring that the very short comment period has not afforded us sufficient time to fully consider precisely how these controls would work or what their impact would be. We hope that the next proposed rule from BIS will bear little resemblance to the

current proposed rule, in which case that may be a good time to discuss more palatable solutions in more detail.

It may be possible, for instance, for these controls to be crafted as Part 744.6 restrictions on activities of U.S. persons. Like the existing Part 744.6 controls, the proposed rule targets a broad set of items but only when used in very narrow ways, though ways that would have a profoundly dangerous impact. The existing Part 744.6 controls target transactions involving *any item* intended for the proscribed end-uses: nuclear explosive devices, missiles, or chemical or biological weapons. That is a good model for the cybersecurity controls, because nearly any software product or method can be used maliciously to steal data or invade privacy, as we hope we adequately demonstrated in the preceding sections. These are not controls that would be effective by attempting to spell out particular capabilities or technical characteristics. Any effort to target specific items will always be both underinclusive (by failing to keep up with new ways that bad actors operate) and overinclusive (by sweeping in legitimate defensive tools), and it would be a mistake to underestimate how innovative cyber operators can be in coming up with completely new ways of achieving their goals.

Furthermore, controls modeled on Part 744.6 make sense here because they are based on knowledge. As discussed at length in the preceding sections, the only distinction that can be made between many types of necessary defensive cyber products and malicious tools is the intent of the user. That end-use intent is exactly what Part 744.6 targets. A control regime based on knowledge and end-use will be more adaptive and more effective—and less of a drain on regulatory and enforcement resources—because it has the advantage of focusing directly on the actual ends (stopping malicious cyber activity) rather than employing a flawed focus on the means (systems, software, and tools that are capable of being used for both malicious and defensive purposes). Moreover, under this approach, BIS would not have to struggle to constantly revise the regulations to account for the new technological developments that are a constant in this industry. BIS is likely to always lose that race; and it is probably not a race they want to be in. Part 744.6 requires every manufacturer, exporter, trader, shipper and facilitator to conduct due diligence in any transaction involving red flags indicating possible unlawful end-uses. The people that live in this world are the most well-suited to spot the threats. Even more, cybersecurity companies have the most at stake here and would be active partners in this effort, provided that the regulatory regime takes account of how this industry works. Their business relies completely on their reputation with their customers and the integrity of their systems. If their products were diverted to malicious groups, they would lose their customers' trust and lose their business. A regime focused on due diligence rather than a constant churn of pointless license applications would make sense. And it would be transformative from a law enforcement perspective: a panopticon of cybersecurity companies always watching for diversion would be exponentially more effective than a BIS licensing officer wondering why he still hasn't seen an application from the bad guys.

A control regime structured like Part 744.6 would match the global nature of this threat. Rather than crafting different country-based licensing policies when malicious cyber threats emanate from anywhere and everywhere, this approach focuses on the particular threat profile (intent and capability) of the end-user. Again, rather than putting the responsibility on a BIS licensing officer to decide whether a sale to a little-known company in Estonia, for example,

should be permitted, and rather than making BIS constantly update its geographical licensing policies based on new threat intelligence, it would make more sense for the people on the ground to make that call, at the risk of facing liability, and losing their business. In cases when the government does have the relevant information to play a useful role, Part 744.6(b) has a built-in provision for special controls upon notice to the person concerned.

This type of control would also have the desired scope: it would cover activities by foreign nationals in the United States, U.S. citizens and residents anywhere in the world and U.S. companies and their foreign branches. Furthermore, Part 744.6 controls can extend to support activities such as financing and other facilitation, as well as performing any contract, service or employment that the U.S. person knows will directly assist in the proscribed activity.⁸³

The Coalition welcomes a conversation about whether controls modeled on Part 744.6 would make sense in this context. However, because of the unduly short comment deadline, the Coalition has not yet made a final determination about whether it would fully support this type of construct. Of course, the Coalition would also have to judge any such proposal on its detailed language, so we look forward to a subsequent proposed rule from BIS that takes a more thoughtful approach.

B. “Band aids” That May Patch a Hole But Will Not Fix the Fundamental Problem With the Proposed Rule

The Coalition hopes that BIS will not delay productive conversations on this topic by trying to fix its broken rule. Malicious cyber-attacks are a clear and present danger to our national security and economic competitiveness, and the scarce resources behind this effort should not be spent focusing on an approach that will not work. Nonetheless, to demonstrate the efforts the Coalition has undertaken to think about whether it would be possible to fix the current proposed rule, we lay out some of those ideas below. These proposals would help make the proposed rule somewhat less harmful, but they will not make it any more effective.

1. License Exception for Legitimate Security End-Uses

It may be possible to craft a broad license exception for legitimate cybersecurity end-uses, which could significantly decrease the negative side-effects of the proposed rule. Of course, such a broad license exception would not make the controls any more effective in targeting the malicious conduct for which they were ostensibly designed—the only way the Coalition is aware of to accomplish that goal would be to reshape the prohibition itself around intent and end-use rather than sticking with a strict liability item/destination framework. But it still may be worth thinking about how a broad license exception like this would work.

There are already examples in the EAR of broad license exceptions based on end-use. For example, License Exception CIV authorizes exports and reexports of certain items on the CCL that are controlled for national security (NS) reasons only and destined to civil end-users for civil end-uses in certain listed countries.⁸⁴ If a similar license exception could be created to

⁸³ Section 744.6(a)(1)(ii) and (a)(2)(i) and (ii).

⁸⁴ Section 740.5.

allow legitimate cybersecurity companies to continue to operate unrestricted by a licensing burden (including deemed exports), such a proposal may satisfy many of the Coalition’s concerns. Unlike License Exception CIV, however, such a provision could not contain significant geographical limitations, given the global nature of the cybersecurity world.

A broad license exception of this type could be based on security or defense, data protection, or similar end-uses. For example, it could include language such as “software designed to add security or benign functionality beyond the original intent of the designer of the system or software that it enhances.” Another possibility would be a license exception for end-uses or added functionality with the knowledge and consent of the authorized user, system administrator, or network owner. In either case, like License Exception CIV, such a provision could impose liability if the person “knows” the item is intended for malicious end-uses or end-users. That would look somewhat similar to the Part 744.6 controls discussed above, but there would still be a need to create an underlying prohibition that makes sense, which is why we believe that removing these systems, software, and technology from the construct of the CCL, and instead working this control regime into Part 744.6 in the first place, would be the best approach.

Any attempt to make such a license exception too specific would probably not be workable. For instance, license exceptions for penetration testing and red teaming (where a group of security professionals accesses an organization’s system in ways similar to malicious actors to test its defenses) would again run into the problem of becoming almost immediately obsolete. It is simply not feasible to try to draw up specific exceptions for products and services available today. Even a fully inclusive list of all products and services available today cannot account for cybersecurity defenses that have not yet been invented and cannot today be contemplated. As attacks evolve so must defenses, and such a limited approach would undoubtedly hamper innovation in new defensive capabilities that are unknown today but may be critical tomorrow.

2. License Exception Based on End-User Statements

Another potential model for a broad license exception could be one requiring certain assurances from the end-user. For example, License Exception TSR permits exports and reexports of certain technology and software controlled for NS reasons only, but again only when destined to certain countries.⁸⁵ License Exception TSR requires a written assurance in advance from the consignee or importer that it will not, without BIS authorization, engage in certain prohibited exports or reexports of the technology or software. This model could be applied in the cybersecurity context by requiring an assurance regarding unauthorized re-transfers, end-uses without the knowledge and consent of the authorized user, system administrator, or network owner, or limited end-use only for the purpose of protecting the end-user’s own system. However, again, any such license exception would not be workable if it contained significant geographical limitations. And an even more significant limitation on the effectiveness of such a requirement would be the reluctance of non-U.S. researchers—often working as volunteers—to sign such a limitation that is presented to them by a party with whom they may not have a contractual or other formal relationship.

⁸⁵ Part 740.6.

3. License Exception for Transfers Among Parties to a Contract or Non-Disclosure Agreement

Another idea would be to create a license exception that would permit transfers to customers or third parties with which a U.S. company has a contractual relationship, non-disclosure agreement (“NDA”), or information sharing agreement. That would address a sizeable portion of the cybersecurity business, but it would cut off a critical population of third-party researchers and collaborators who will only work with U.S. companies on an informal basis. Because many of those individuals will never be convinced to sign a piece of paper, this type of solution will never allow the U.S. cybersecurity industry to stay on the cutting-edge. If there are other ways to address exchanges with those informal business partners, e.g. some sort of basic reporting requirement, it is conceivable that this type of provision could constitute a partial solution, but, at the very least, it would have to be in conjunction with large carve-outs for internal company operations (e.g. deemed exports and intracompany transfers, discussed below).

4. License Exception for Activities Compliant with Software Terms and Conditions

Some outside the Coalition have raised the idea of creating a carve-out for activities conducted within the scope of software license terms and conditions. The idea would be, for example, that it should not be prohibited for a cybersecurity company to probe or add functionality to an off-the-shelf program like Microsoft Word in a way that does not violate the terms and conditions imposed by Microsoft on Word users or if allowed by the authorized user, system administrator, or network owner. In contrast, those terms and conditions may in theory prohibit the type of activities that malicious actors would engage in, so those activities would remain prohibited. However, such a solution is not likely to be workable in most instances, because software terms and conditions generally do not contain prohibitions that would be relevant in this context. Instead, they tend to simply disclaim any warranties based on misuse or alteration of the product, which would not be helpful in distinguishing malicious activity from legitimate defensive activity. And, even where they are restrictive enough to prohibit malicious activity, they may do so in a way that also prohibits benign software innovation and addition of functionality that the authorized user, system administrator, or network owner desires. Therefore, the Coalition does not view this type of proposal as being particularly promising, but it may be worth exploring in more detail at a later date.

5. Carve-Outs for Deemed Exports and Intracompany Transfers

In conjunction with some sort of broad carve-out for customer and third-party transfers like the one discussed in Section VII.B.3, above, a broad permissive provision related to deemed exports and intracompany transfers would relieve a significant portion of the Coalition’s concerns regarding the proposed rule.

6. License Exception ENC Framework

One example from the existing encryption controls that could provide a basic theoretical framework is License Exception ENC, which authorizes exports and reexports of certain encryption items to certain end-users in certain countries for certain end-uses without the submission of encryption registrations, classification requests, self-classification reports or sales

reports.⁸⁶ License Exception ENC is far more restrictive than any viable counterpart could be for cybersecurity items. The geographical restrictions in particular would be problematic, but any item type, end-user or end-use limitations would also have to be carefully crafted to account for the nuances of how the cybersecurity sector works. Furthermore, any registration or reporting requirement would have to take account of the constantly-changing nature of cybersecurity technology, and could not, for instance, require re-submission with each change in functionality. Nor could it mandate an unduly burdensome level of disclosure, particularly regarding certain sensitive third-party relationships and current vulnerabilities. Importantly, any waiting period (e.g. like the 30-day waiting period under ENC) would likely make such a provision unworkable. Overall, while License Exception ENC may provide a basic theoretical model for how a cybersecurity provision may work at a macro level, the details would have to be significantly adapted to the realities of this industry.

It is also important to note that this type of hands-on regulatory framework may not be feasible for smaller companies, researchers and independent operators—a vital part of the U.S. cybersecurity community—who would not have the resources to comply. Creating barriers to entry of this kind generally leads to stagnation of the market and hinders innovation.

7. Note 4 to Category 5, Part 2

Another possible model for cybersecurity items is the decontrol available for encryption items in Note 4 to Category 5, Part 2. Note 4 states that Category 5, Part 2 does not apply to items using “cryptography” that do not have certain “primary functions” (such as information security; a computer; sending, receiving, or storing information except in certain circumstances; or networking), as well as certain other requirements. A similar test related to “primary function” could be proposed for cybersecurity items (for example, “intrusion software, whose primary function is the protection of data or systems or that is intended to be used with a network owner’s or system administrator’s knowledge and consent”).

8. Less Tightly Controlled ECCNs

Another potential model could be the less tightly controlled ECCNs covering certain encryption items.⁸⁷ Encryption items under these ECCNs are only controlled for anti-terrorism (AT) reasons and therefore can be exported without a license to most destinations. A cybersecurity analog could include items like mass market products, benign or authorized end-uses, etc.

⁸⁶ Part 740.17.

⁸⁷ For example, encryption items that fall under “5x992” ECCNs include those with weak encryption (below 56 bits for symmetric algorithms and below 512 bits for asymmetric algorithms); limited encryption functionality (authentication, access controls, digital signatures, financial data, “fixed” compression or encoding, etc.); unused or disabled encryption functionality; and mass market items (publicly sold without restriction, where the cryptographic functionality cannot be easily changed by the user and it is designed for installation without support).

VIII. CONCLUSION

Given all of the fundamental flaws and unworkable provisions in the proposed rule identified and discussed above, BIS should go back to the drawing board and begin again to consider how to control malicious cyber items from a clean slate. As described in detail above, the current proposed rule is fundamentally flawed and should not serve as the starting-point for any future proposed rule. To implement the current proposed rule would be devastating to U.S. cybersecurity. We hope that BIS will view this first proposed rule and the comments received in response as a valuable learning exercise that demonstrated how damaging and ineffective the proposed rule would be, as well as a framework from which to approach future Wassenaar discussions.

Because critical defensive products and methods are technically indistinguishable from malicious tools, because of the global nature of the workforce, and because these technologies are changing so rapidly, BIS should not continue to pursue controls that are based on the classification of the item (i.e. its functional characteristics) and the country of destination. Any future control regimes that are proposed should focus on the intended end-use, since that is the only way of separating defensive from offensive tools. Such a control regime would also have to take account of the entire cybersecurity community—including established companies, start-ups, academics, and independent researchers—because fencing off any part of this community would have devastating effects on innovation and on U.S. companies' ability to stay ahead of the global threat environment. Furthermore, any workable controls cannot contain significant geographic restrictions, because some of the most risky countries from a threat perspective are also the most critical places for U.S. companies to be able to protect themselves adequately. Finally, any cybersecurity controls must not impose any requirements that involve waiting periods for critical activity, because this sector operates in seconds and minutes, not weeks and months.

The Coalition would be pleased to offer whatever additional support it can to help the U.S. government craft a regulatory regime that will work. We hope that some of the ideas we have raised in Section VII.A will be a useful starting point for a new proposed rule, but, again, we will need more time to consider how any controls modeled on Part 744.6 or other proposed modifications or approaches would work in practice in our industry before we can express any definitive opinion. It is important that we work together to get this right, for the sake of our collective national security and future economic competitiveness, and to find a way of countering the very real threats that exist in a way that will be effective. If you have any questions please do not hesitate to contact Meredith Rathbone (202-429-6437; mrathbone@steptoe.com), Stewart Baker (202-429-6402; sbaker@steptoe.com) or Alan Cohn (202-429-6283; acohn@steptoe.com).

Respectfully submitted,



Meredith Rathbone
Stewart A. Baker
Alan Cohn
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, NW
(202) 429-3000
mrathbone@steptoe.com
sbaker@steptoe.com
acohn@steptoe.com

On behalf of the following members and supporters of the Coalition for Responsible Cybersecurity:

IONIC SECURITY INC.
Adam Ghetti, CTO
Robert Ball, Chief Legal Counsel
Ryan Speers, Director Applied Research

SYMANTEC CORPORATION
Cheri F. McGuire, Vice President, Global Government Affairs & Cybersecurity Policy

FIREEYE, INC.
Shane McGee, Chief Privacy Officer
Orlie Yaniv, Director, Government Affairs and Policy

SYNACK, INC.
Mark Kuhr, CTO

TRAIL OF BITS, INC.
Dan Guido, Co-Founder and CEO

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-3jnv
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0210

SET Comments from Japanese private sctor METI

Submitter Information

General Comment

See attached

Attachments

SET Comments from Japanese private sctor METI

Comments from Japanese private sector

TO:

Ms. Catherine Wheeler

Director, Information Technology Control Division

1-202-482-0707

Catherine.Wheeler@bis.doc.gov

FROM:

Office for IT Security Policy,

Commerce and Information Policy Bureau,

Ministry of Economy, Trade and Industry, Japan

Masahiro Uemura (Director), Takuma Maeda (Assistant Director)

TEXT:

The Office for IT Security Policy, Ministry of Economy, Trade and Industry (“the Office”) would like to provide the following comments given by JPCERT/CC, Japanese CERT of which the Office is in charge, and JNSA: Japan Network Security Association, a Japanese association of information security enterprises, during the consultation between the Office, IPA: Information-technology Promotion Agency, JPCERT/CC and JNSA. The Office would like to ask for positive consideration on this matter.

The Comments from JPCERT/CC

(1)The concern regarding the ways to describe in FAQ
BIS FAQ shows that BIS is taking care so that the flow of information etc. on the zero-day vulnerabilities for security maintenance purpose is not subject to control. But this information is also used as a component of intrusion software which is subject to control. Therefore there is a concern that the careful interpretation of FAQ leads to security-oriented decision which accounts for the halt of information reporting on Japanese device vulnerability discovered by the US researchers to Japan, or the situation that this vulnerability information is exposed to full disclosure without report in advance to Japanese device developers.

JPCERT/CC would like to ask to clearly write down on the main text of EAR that the vulnerability information for security maintenance purpose is not subject to control so that the flow of vulnerability information will not depend on the interpretation of FAQ.

(2)The concern for disturbing international coordination of vulnerabilities JPCERT/CC arranges distribution/forwarding of information concerning the devices of companies whose base are located in other Asian countries from American researchers or CERT/CC to Asian companies. JPCERT/CC would like to ask for consideration so that the flow of vulnerability information to other Asian countries than Japan will also not be disturbed.

(3) The Concern regarding the handling of zero-day vulnerabilities of Japanese devices found in the US.

It is favorable from the security maintenance perspective that when the malware abusing the zero-day vulnerabilities of software products of Japanese companies is found in the US. the malware sample is provided to Japanese companies in order to take vulnerability countermeasures. The concern is that if those malwares are decided to be subject to EAR, then the malware samples will not be exported and necessary countermeasures will not be taken.

The Comments from an Industry Association

Japan Network Security Association (JNSA), Social Activities Committee

- Please explicitly state that the activities such as gathering, investigating and analyzing information in order to maintain the security of information systems is outside of the scope of this control

- Please explicitly state that programs which seek to carry out forensic activities in aims to maintain security (and not legal investigations) for domestic enterprises with headquarters, branch offices or subsidiaries overseas (including in the U.S.) are not eligible.

-Broad scope of the “Intrusion and Network Penetration Items” definition-

Legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using Intrusion Software, should not be considered within the scope of this control.

-Interpretation of “IP Network Surveillance Systems” under the areas of control- Much, if not all, of the equipment which may be utilized in surveillance systems consists of ordinary, commercial-off-the-shelf, information technology hardware and software, which is necessary for carrier class IP network operations. For example, carrier class IP networks typically include core routers. These core routers may implement port mirroring to direct data to a monitoring platform. The monitoring platform may perform deep packet inspection to screen for malware and/or provide quality of service. It is very important that general purpose carrier class IP networking equipment and components should not be classified high restrictive export control classifications, requiring export licensing which under the current regulations can be exported under a license exception.

-Chilling Effect on Security Research- Implementation of the Wassenaar2013 Plenary Agreements already has had negative effects on legitimate vulnerability research and, hence, the ability of companies to protect their own networks. Security researchers in European countries, where the rules already are effective, have reduced or discontinued their contributions to programs which reward discovery of security flaws, out of concerns with respect to the scope of these controls.

End

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-3mft
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0211

ITI Comments on BIS Proposed Rule on Intrusion Software - 20 July 2015

Submitter Information

General Comment

See attached

Attachments

ITI Comments on BIS Proposed Rule on Intrusion Software - 20 July 2015

July 20, 2015

Ms. Catherine Wheeler
Director, Information Technology Control Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Dear Ms. Wheeler:

The Information Technology Industry Council (ITI) welcomes the opportunity to provide its views on the proposal by the Bureau of Industry and Security (BIS) to implement stricter export controls on certain “cybersecurity” products – namely those interacting with “intrusion software” – identified in 2013 by the Wassenaar Arrangement. While we support the human rights objectives inspiring this effort under Wassenaar, we have significant concerns regarding the commercial and security implications of this proposed means of achieving them. We look forward to working with you and your colleagues to address these concerns.

ITI is the global voice of the information and communications technology (ICT) industry. Our members include the world’s leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI advocates policies that advance industry leadership in technology and innovation, open access to new and emerging markets, promote e-commerce expansion, protect consumer choice, and enhance the global competitiveness of its member companies.

A central element of our advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not just to the ICT sector but to the global economy as a whole. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to conduct research and development, design and manufacture goods, and market and distribute products and services to their customers. U.S. and global ICT companies also have a long history of exchanging security-related information across borders with users, customers, governments, and other stakeholders, which helps them protect their own systems and maintain high levels of security for the technology ecosystem as a whole.

The Obama Administration has consistently recognized the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. Earlier this year, President Obama issued [Executive Order 13691](#), which, among

other things, states that “private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.” We are concerned that the proposed rule could undermine this key Administration principle and severely complicate the ability of companies in all sectors to protect and enhance their security.

As an initial matter, the proposed rule presumes clear lines of demarcation between “intrusion software” (not controlled) and “software that generates, delivers, or communicates with intrusion software” (controlled). However, subject matter experts do not agree on whether this line exists in reality or, if it does, exactly where it lies. The natural consequence for compliance-driven exporters would be to assume a very conservative position by “playing it safe” and assuming that large volumes of software/technology would be controlled. The natural consequence for BIS would be unpredictable (but likely large) volumes of license applications.

Similarly, the overall breadth of the draft measure would mean that companies could be required to apply for and obtain literally thousands of export licenses to cover the vast range of information-sharing and other security-related activities that they undertake involving the movement of data across borders (in areas such as product development, security testing and research) and the proper securing of their own and their clients’ information and networks. It would be extremely burdensome and costly for individual companies to prepare license applications and for BIS to review and rule on them. It would also be extraordinarily time-consuming. Months could pass between the time that the need to share threat information arises and the time permission to do so is granted. Meanwhile, potential vulnerabilities could be exploited many times over.

The proposed measure would be harmful even at the level of individual companies as it relates to their own internal data sharing and cybersecurity operations. A single company might need to obtain large numbers of licenses for its headquarters to share certain security information, software and tools with overseas affiliates or use certain products to insure the security of its internal network. Even domestically, a manager at headquarters might need to obtain a license to walk down the hall and discuss certain security issues or development of new tools with a team member who is a national of a country other than the United States or Canada.

In addition, there are potentially broader international ramifications of pursuing such policy approaches. Whatever the rationale, the broad scope of the proposed rule would be seen as the imposition of government restrictions on cross-border data flows. Such rules would provide a precedent for other governments to expand their own limitations on the flow of information across borders, including on the basis of “security,” to the detriment of global trade and U.S. companies operating in those markets.

In sum, BIS’ proposed rule would not only impose tremendous costs on some of the United States’

leading innovators and job-creators. It would also directly undermine efforts to achieve the Administration's objectives for enhancing commercial information security, both of the companies covered by the regime and the global ICT ecosystem generally.

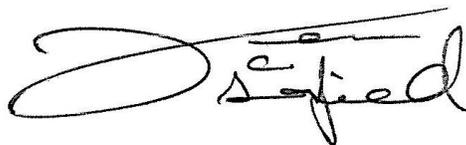
We urge BIS to cease consideration of this harmful proposed measure and immediately engage the U.S. ICT industry and other stakeholders in detailed consultations regarding how best to achieve the human rights objectives of the Wassenaar Arrangement without compromising the security objectives of both the Administration and the ICT industry. Such consultations would allow government and industry to discuss preferable steps to take, including, but not limited to:

- establishing a working group of technical experts from government and industry to systematically address the technology and cybersecurity considerations at issue;
- providing for a self-executing license exception mechanism under section 740 of the Export Administration Regulations (EAR) that does not include reporting requirements and is structured to enable exporters to export, re-export, and transfer (including in-country transactions) systems, equipment, components, technology, and/or software for internal company use worldwide;
- maintaining relevant provisions of the encryption (ENC) exception, to avoid placing unnecessary burdens on companies' security operations and innovation capabilities; and
- providing for an "intra-company license exception" that would allow for information sharing, internal company use of security products, and end user controls that do not block legitimate permissible uses.

We would be pleased to discuss other ideas for achieving our shared objectives in this regard.

Thank you for your consideration of these comments. We look forward to working with you and your colleagues further on these important issues.

Sincerely,



Dean C. Garfield
President and CEO

cc: Kevin Wolf, Assistant Secretary for Export Administration
Matthew Borman, Deputy Assistant Secretary for Export Administration
Hillary Hess, Director Regulatory Policy Division, Office of Export Services

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7r-r5br
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0212

Alliance for Network Security Comments on WA 2013 Cyber Rule

Submitter Information

General Comment

See attached

Attachments

Alliance for Network Security Comments on WA 2013 Cyber Rule



July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49) Published in 80 Fed Reg 28853 on May 20, 2015

Dear Sir/Madam:

On May 20, 2015, the Commerce Department's Bureau of Industry and Security ("BIS") published a Proposed Rule in the Federal Register entitled *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items* (RIN 0694-AG49). See 80 Fed Reg 28853. Because the Proposed Rule is written broadly, could have significant unintended consequences, and could pose a major burden upon industry and BIS, the Alliance for Network Security is submitting these comments with the recommendation that BIS postpone the Proposed Rule's implementation and significantly narrow its scope.

The Alliance for Network Security ("ANS") is an industry association comprised of Alcatel-Lucent, Cisco Systems, Inc., DataDirect Networks, Google Inc., Hewlett-Packard Company, Hitachi Data Systems Corp., Intel Corp., Juniper Networks, Inc., Microsoft Corp., Micro Focus, Qualcomm Inc., Rockwell Automation, Inc. and Symantec Corporation. For over fifteen years, ANS has advised the United States and foreign governments with respect to export and import controls on cryptography. We appreciate this opportunity to provide comments with respect to the Proposed Rule on Intrusion and Surveillance Items. We understand that BIS primarily is interested in the following subjects:

1. *How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:*
 - a. *How many additional applications would be for products that are currently eligible for license exceptions?*
 - b. *How many additional applications would be for products that currently are classified EAR99?*
2. *How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?*
3. *Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.*

4. *How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?*

The ANS members respectfully submit that the number of export (including deemed export) license applications they would be required to submit is difficult to determine for several reasons. First and foremost, this is a new control, so ANS members do not have prior experience that is particularly relevant. Moreover, the number of export licenses required will depend on the interpretation of key provisions in the Proposed Rule. ANS member companies currently estimate that the number of export license applications required may be numbered into the hundreds for some ANS member companies, and may be numbered into the thousands of export license applications for some of the largest ANS member companies with large, globally-based security teams. We believe the estimated number of licenses represent an unknown, but likely a significant licensing burden for BIS. Having to seek export licenses means that the “real time” ability to identify and mitigate the impact of bad actors against customers would cease for U.S. companies, while global competitors would not be under similar constraints. In addition, export licenses also could not be obtained in advance for every situation for which export authorization may be needed, since the specific controlled technology or software to be exported or reexported, and the identity of the foreign nationals, entities, and destinations with whom the items will be shared, generally will not be known in advance. License delays or the inability to obtain needed licenses will put at risk millions of ANS customers, including the U.S. Government, and critical U.S. infrastructure. Therefore, the first section of these comments will focus on these key interpretive issues.

The ANS members also respectfully submit that the implementation of the Wassenaar 2013 Plenary Agreements already has had negative effects on legitimate vulnerability research and hence the ability of ANS members to protect their own networks. The second section of these comments will focus on this subject.

I. Key Provisions in the Proposed Rule That Affect the Export License Requirements

The Proposed Rule contains two key provisions that affect the export license requirements of ANS member companies. The first, dealing with Intrusion Items, is addressed in Section A of this letter. The second, dealing with Surveillance Items is addressed in Section B of this letter.

A. Intrusion Items and Network Penetration Testing

At first reading, the Proposed Rule appears to be susceptible of an interpretation that is relatively narrow with respect to the scope of controlled intrusion items. Neither the security vulnerability itself, nor the “intrusion software” that exploits the security vulnerability, would be controlled under the Proposed Rule. Rather, the Proposed Rule would control systems, equipment,

components (4A005) and software (4D004) that are specially designed or modified for the generation, operation, or delivery of, or communication with, “intrusion software”. The Proposed Rule also would control technology (4E001.a) if required for 4A005, 4D004.a (if required for 4A005 or 4D004) and if required for 4E001.c.

The interpretive issue that concerns the ANS member companies is addressed in the Supplementary Information section of the Proposed Rule at page 28854 under the sub-heading, Scope of the New Entries, which reads in relevant part as follows:

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.

The ANS members suggest that the scope of control on intrusion items should be strictly limited to platforms for launching attacks and technology required for the development of those platforms. Examples include platforms developed and marketed by companies like Gamma International and HackingTeam.

Both companies are highly secretive, but the limited publicly available information suggests that FinFisher’s FinSpy and HackingTeam’s Remote Control System (RCS), respectively, are suites of equipment, software and services used for surveillance and monitoring. In both suites, there is a specific application that acts as the administrative command center, listing and managing the recovered information. FinFisher also offers a hardware platform with pre-loaded software for the operation and delivery of intrusion software.

On the other hand, legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using Intrusion Software, should not be considered within the scope of this control. Among the network penetration testing programs that are widely used by ANS member companies are Metasploit and Nessus. Both of these products are available in versions that qualify for decontrol under the Wassenaar General Software Note (because they are publicly available) and/or the Wassenaar Cryptography Note (because they are mass market). Hence, other Wassenaar member countries would not control either of these software programs. However, if we look at Metasploit, for example, the Proposed Rule appears to control one (Metasploit Pro – mass market) but not the other (Metasploit Framework – publicly available). Therefore, it is especially important that BIS must not interpret ECCN 4D004 in a manner that would implement controls on general purpose network penetration testing products. We understand

that the export control authorities of Japan have reached agreement on a similar interpretation with its affected industry in Japan. [See](#) Figure 1.

B. Surveillance Items and “Combined” Equipment

Likewise, at first reading, the Proposed Rule appears to be susceptible of an interpretation that is relatively narrow with respect to the scope of controlled surveillance items. Only products that perform *all of the functions listed* are controlled under the new entry (5A001.j).

Upon closer inspection, however, much of the equipment that may be utilized in surveillance systems consists of ordinary, commercial-off-the-shelf, information technology hardware and software, which is necessary for carrier class IP network operations. For example, carrier class IP networks typically include core routers and firewalls. The firewalls might perform deep packet inspection of communications data to screen for malware. It is not clear from the Proposed Rule that screening for malware falls within one of the exceptions to the proposed classification, such as being related to Quality of Service or Quality of Experience.

In addition, the proposed entry contains several vague terms that would benefit from clear definitions. For instance, proposed j.2.b pertains to “Mapping of the relational network of an individual or of a group of people.” It is not clear what constitutes or defines a “group of people.” Similarly, the term “hard selector” is defined so that it could relate to “group affiliations” of individuals. Neither “group of people” nor “group affiliations” is defined and could be interpreted as applying to the screening of data related to persons affiliated with a specific criminal hacking collective, a foreign military intelligence unit, a terrorist organization, or other potentially nefarious group, uses of screening traffic we believe should not be proscribed. This is an important enough point that we think it needs to be addressed in the regulations themselves, as opposed to in an FAQ on the BIS website or another less formal method.

Another concern arises from an interpretive issue in the Supplementary Information section of the Proposed Rule at page 28854 under the sub-heading, Scope of the New Entries, which reads in relevant part as follows:

[T]he Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry. (Emphasis added.)

We think that the addition of this language with respect to what the exporter “intends” is neither consistent with the plain language of the Wassenaar text nor necessary to accomplish the purpose of this control. The Wassenaar text is listed in the conjunctive, so that only systems having all of the functions specified therein are subject to control. Furthermore, Section 764.2(h) of the EAR

provides enforcement authority in cases where the exporter's conduct constitutes "evasion" of the requirements of the EAR.

We have the same concern with the "Related Controls" language under ECCN 5A001 on page 28861, which reads in relevant part as follows:

However, such equipment may not be sold separately with knowledge that it will be combined with other equipment to comprise a system described in new paragraph ECCN 5A001.j.

It is very important that general purpose carrier class IP networking equipment and components should not be classified under ECCN 5A001.j, even if, somewhere else in the network infrastructure, there may be a network surveillance capability.

BIS repeatedly has stressed that this is not an end-use control. If there is any item unique to a surveillance system, it is the software which performs the functions described in sub-paragraphs j.2.a and j.2.b.

We respectfully suggest that, if anything, then only items which perform the functions described in sub-paragraphs j.2.a and j.2.b should be controlled based on the "intent" to combine them with other items controlled under this entry.

II. Proposed Rule's Chilling Effect on Security Research

Implementation of the Wassenaar 2013 Plenary Agreements already has had negative effects on legitimate vulnerability research and, hence, the ability of ANS members to protect their own networks. Security researchers in European countries, where the rules already are effective, have reduced or discontinued their contributions to ANS members' programs which reward discovery of security flaws (sometimes referred to as "bug bounties"), out of concerns with respect to the scope of these controls.

For example, concerns with respect to the impact of the Wassenaar 2013 Plenary Agreements on the security vulnerability research community have been expressed by Sergei Bratus, Michael Locasto and Anna Shubina in a seminal paper entitled *Why Wassenaar Arrangement's Definitions of "Intrusion Software" and "Controlled Items" Put Security Research and Defense At Risk*. (See <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.) Bratus and his co-authors state that use of the phrase, "modification of the standard execution path of a program or process in order to allow the execution of externally provided instruction," as a qualifying factor, even when subject to the limitation that the modification must be in conjunction with avoiding detection of 'monitoring tools' or defeating 'protective countermeasures', is overly broad, resulting in non-malicious programs falling under the rubric of Intrusion Software. The authors offer as their primary example Microsoft's Detours software library which, according to Microsoft, "intercepts Win32 functions by re-

writing the in-memory code for target functions.” Bratus asserts that many programs utilize Detours in order to perform live updates to programs, and because of the requirements that the memory be located in order to be adjusted in order for the updates to take place, they must effectively “defeat ‘protective countermeasures’” (specifically, Address Space Layout Randomization) as described in the Proposed Rule. Bratus also expresses concern that the term “defeating ‘protective countermeasures’” could encompass programs performing tasks such as jailbreaking used to defeat sandboxing, further asserting that there are many legitimate reasons to “defeat ‘protective countermeasures’”. Bratus and his co-authors also explain how the Proposed Rule could hinder the development of a relatively new computer science concept known as Automated Exploit Generation (AEG), involving the automated discovery and testing of vulnerabilities in programs, allowing for automated generation of test exploits as they are developed to determine the severity of discovered bugs. They go on to suggest that, left unimpeded by the Wassenaar 2013 Plenary Agreement, AEG could become an important software verification tool, almost akin to a debugger.

These views are not uniformly shared within the security vulnerability research community. For example, Colin Anderson has offered an alternative interpretation in a paper entitled *Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies*. (See https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156a_e1m6b9vib.pdf.) Anderson asserts that the Wassenaar 2013 Plenary Agreement, properly understood, is narrowly tailored to target the intended offerings from companies like FinFisher and HackingTeam. Anderson also describes how FinFisher and RCS differ from products such as Metasploit and “jailbreaks”, which in his view are not subject to the Wassenaar 2013 Plenary Agreement.

Regardless of whether one subscribes to the Bratus view, or the Anderson view, the fear, uncertainty and doubt surrounding the scope and effect of the Wassenaar 2013 Plenary Agreements has resulted in a reduction in the reporting of security vulnerabilities to ANS member companies. The BIS could address this in part by reference in the final rule to the provisions governing published information, information resulting from fundamental research, and educational information set forth in Section 734.7, 734.8 and 734.9 of the EAR. The BIS also has provided, and should continue to offer, helpful guidance periodically on its web site. However, resonances of the concerns raised by Bratus and his co-authors still reappear, from time to time. See, e.g., articles published by David Perera in *Politico* on June 2 and June 8, 2015. Certainly, BIS can, and should, continue posting FAQs on its website, addressing specific techniques of concern, such as “fuzzing” and other techniques.

In addition, BIS may wish to post on its web site flow charts illustrating the decision tree structure of the final rule (not only for intrusion items, but also for surveillance items described in the Proposed Rule). These flow charts would assist exporters in their understanding of some of the conclusions BIS has reached in its FAQs.

As an example of an area that requires further clarification, to the extent that BIS intends to maintain licensing requirements for rootkits and zero-day exploits, it should provide specific definitions for those terms and explain the basis for such controls. (ANS member companies are of the view that rootkits and zero-day exploits should fall within the definition of "intrusion software," and therefore would *not* be controlled and therefore would *not* require a license under this rule.)

Although admittedly difficult, ANS members respectfully submit that it nevertheless should be possible to differentiate between network penetration testing tools and Intrusion items. We look forward to working with BIS toward that shared objective. As a place holder, we would recommend that BIS consider adopting a Commodity Interpretation in Section 770.2 of the EAR, along the following lines:

(n) Interpretation 14: Intrusion items described in ECCNs 4A005, 4D004 and 4E001.c do not control hardware, software or technology for network penetration testing. Exporters are advised to review the specific text of these ECCNs, in conjunction with the exemption for publicly available technology in Section 734 of the EAR as well as the General Software and Technology Note in Supplement No. 2 to Part 774 of the EAR.

This text also might serve as a basis for discussion of additional refinements to the definition of "intrusion software" during the Wassenaar Dual Use List Review in 2016.

However, ANS members have another, deeper and broader, concern. Many companies choose not to publish or otherwise make publicly available information concerning security vulnerabilities or the techniques they are using to safeguard their own and their customers' products and networks. Nevertheless, they need to share information with respect to such vulnerabilities and techniques between and among their foreign subsidiaries, foreign national employees, and even with other companies and entities facing similar issues.

Indeed, Executive Order 13,691 specifically articulates this information sharing requirement in Section 1, Policy, which reads in relevant part as follows:

Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.

The urgent need for this kind of collaboration is particularly acute where there is an ongoing attack. The vague intent to make available some form of "broad licenses" available is cold comfort to companies who encounter previously unknown advanced persistent threats on an unfortunately

frequent basis. ANS members have observed that their network security professionals responding to attacks simply do not have the luxury of debating the fine distinctions of whether a particular bit of technology or software may be classified under ECCN 4D001, or 4D004, or 4E001, or 5D002, or 5E002, or EAR99, or indeed debating about whether it might need to be added to whatever kind of “broad license” might be contemplated by BIS, before sharing it throughout their network operations centers and taking necessary defensive actions across their worldwide networks.

We recommend that BIS exempt security vulnerability information from the scope of the EAR, when it is shared with the intent to defend against possible attacks. In the alternative, BIS should create a license exception authorizing the export of security vulnerability information, without pre-export review or post-export reporting requirements. Whether described as an exemption or as a license exception, the following activities should be permitted without a license or other approval from BIS:

1. Exports and deemed exports of controlled items relating to intrusion software similar to the current intra-company transfer authorizations for encryption items set forth in License Exception ENC [Section 740.17(a) of the EAR].
2. Exports and deemed exports of controlled items relating to intrusion software when such exports and deemed exports are made:
 - (a) to the producer of the vulnerable product wherever that manufacturer is located and its employees or contractors, or;
 - (b) to any other agent of the vulnerable product’s manufacturer, wherever located; or
 - (c) where the purpose of the export is to report vulnerabilities to manufacturers and to have the vulnerabilities be fixed; or
 - (d) where the purpose of the export is to report vulnerabilities to coordination bodies such as the various CERT organizations around the world and to have the vulnerabilities fixed.
3. Exports and deemed exports of controlled items relating to intrusion software when such exports and deemed exports are made by product manufacturers or their agents to individuals or entities that reported a vulnerability to them. In the alternative, we suggest that exports of controlled items relating to intrusion software should be eligible for export as long as the exporter maintains “effective control” over such items (similar to the current provisions of License Exception TMP).

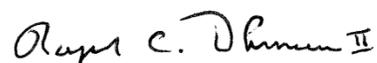
Conclusion

The Wassenaar 2013 Plenary Agreements with respect to intrusion and surveillance items may have significant, negative consequences with respect to important activities of ANS member companies, unless these recommendations are adopted by BIS. To briefly summarize:

- The scope of control on intrusion items should be strictly limited to hardware items for launching attacks and software and technology related thereto, as limited by the General Technology and Software Note and other applicable provisions of the EAR. Legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using intrusion items, should *not* be considered within the scope of this control. BIS and ANS members should work closely together (and with other multi-stakeholder groups like the Commerce Department's National Telecommunications & Information Administration (see <http://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure>) toward the objective of delineating a clear distinction between controlled Intrusion Items and decontrolled network penetration testing products. This distinction should be published first as a Commodity Interpretation in Part 772 of the EAR, and then should be proposed to the participating member states of the Wassenaar Arrangement for recommended adoption in connection with its Dual Use List Review in 2016.
- The scope of components controlled when combined with other items to comprise IP network surveillance systems should be limited to items performing the functions described in sub-paragraphs j.2.a and j.2.b of the new 5A001.j.
- BIS should exempt security vulnerability technology, software and related services from the scope of the EAR, when they are shared with the intent to defend against possible attacks. In the alternative, BIS should create a license exception authorizing the export of security vulnerability technology, software and related services, without pre-export review or post-export reporting requirements to cover technical exchanges intra- and inter-company.

For these reasons, ANS members respectfully request that BIS postpone its implementation of the Proposed Rule so that these issues can be addressed in a second, revised, Proposed Rule.

Sincerely,



Roszel C. Thomsen II

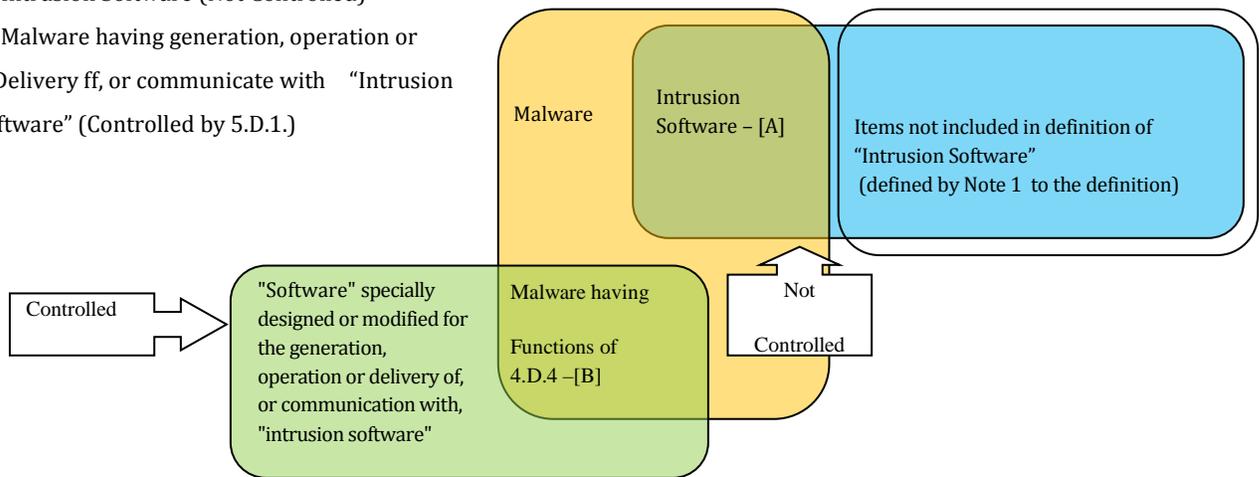
Figure 1: Interpretation of Intrusion Item Controls in Japan

Items		Classification	Related Technology		Related Software	
			Development/ Production	Use	Development/ Production	Use
Intrusion Software		Not Controlled	Controlled (Development) [4.E.1.c.]	Not Controlled	Not Controlled	Not Controlled
Items specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software"	Commodity	Controlled [4.A.5.]	Controlled [4.E.1.a.]	Controlled [4.E.1.a.]	Controlled [4.D.1.a]	Not Controlled
	Software	Controlled [4.D.4.]	Controlled [4.E.1.a.]	Controlled [4.E.1.a.]	Controlled [4.D.1.a]	Not Controlled

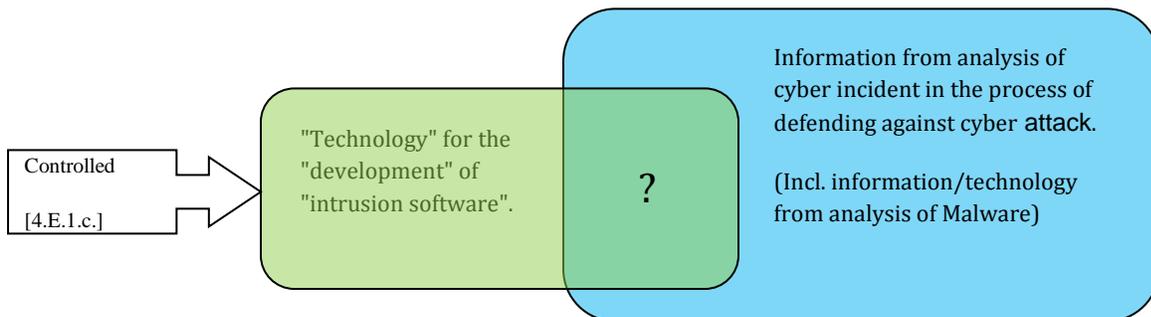
Malware Includes:

[A]- Intrusion Software (Not Controlled)

[B]- Malware having generation, operation or Delivery ff, or communicate with "Intrusion Software" (Controlled by 5.D.1.)



Malware and Intrusion Software



PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7u-xde9
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0213

Intel Corporation Comments to Proposed Rule RIN 0694_AG94 07_20_2015

Submitter Information

General Comment

See attached

Attachments

Intel Corporation Comments to Proposed Rule RIN 0694_AG94 07_20_2015

Intel Corporation
2200 Mission College Blvd.
M/S RNB-5-125
Santa Clara, CA 95054-1537



July 20, 2015

Ms. Catherine Wheeler
Director, Information Technology Control Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

RE: Revisions to the Export Administration Regulations (EAR): Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (Federal Register Notice of May 20, 2015; RIN 0694-AG49)

Intel Corporation is submitting the following public comment in response to the request issued by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") on proposed new regulations for the addition of Intrusion and Surveillance Items to the Export Administration Regulations ("EAR").

1. Intel's Commitment to Cybersecurity

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. Intel is the leading manufacturer of computer, networking and communications products and has over 100,000 employees operating in 300 facilities in 50 countries. Intel develops semiconductor and software products for a broad range of computing applications. These platforms and technology advances are some of the most innovative and complex developments in history, and are now essential to the way we work and live. We envision the role of technology to improve education, energy distribution, government responsiveness and the delivery of health care. It is Intel's mission to create and extend computing technology to connect and enrich the lives of every person on earth.

Security has long been an Intel priority, and is critical to meeting this mission. Indeed, security, along with power-efficient performance and connectivity, comprise the three computing pillars around which Intel concentrates our innovation efforts. A little over a year ago, Intel formed a new business unit to further the security pillar – the Intel Security Group – combining our subsidiary McAfee with other security resources from across Intel to form a single organization focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide.

Intel has shared its position with the U.S. and global governments that we cannot delay in collectively addressing the evolving cybersecurity threats, and indeed our company has been at the forefront of efforts to improve cybersecurity across the compute continuum. As a leading developer and manufacturer of foundational information and communications technology products, we offer a unique understanding of the gravity of our cybersecurity challenges, and the reality that governments, businesses and consumers are facing a cybersecurity threat landscape that has fundamentally changed. Countering these increasingly sophisticated threats to all organizations requires the cooperative efforts of government, industry and non-governmental organization stakeholders working together to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

Intel Security delivers proactive and proven solutions, services, threat intelligence and analytics that help secure systems and networks around the world, allowing users to more securely connect to the Internet and browse and shop the web. Fueled by an award-winning research team, Intel Security creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their

security. Last year, Intel co-founded the Cyber Threat Alliance¹ with other security vendors to drive a coordinated industry effort against cyber adversaries through deep collaboration on threat intelligence and sharing of actionable indicators of compromise, allowing alliance participants to deliver greater security to organizations in the U.S. and worldwide.

2. The Proposed Rule Would Negatively Impact Security, Innovation and Competitiveness

From our vantage point as both a leading global technology innovator and a security company, despite BIS' intention of curtailing the proliferation of malicious and weaponized software, the Proposed Rule requires additional consideration within the context of broader security policy and ecosystem impacts.

Most fundamentally, the Proposed Rule as written would do more to damage rather than improve the cybersecurity of U.S. companies. First, at the macro cybersecurity policy level, the Proposed Rule appears contrary to the thrust of current U.S., and indeed global, cybersecurity policy. The U.S. has consistently defined and referred to "cybersecurity" as the protection and defense of cyberspace². In line with that approach, U.S. policy activities globally have encouraged the robust adoption of cybersecurity solutions in order to make cyberspace more secure. The Proposed Rule is in direct conflict with those long-standing approaches by restricting access to protective security measures required by networks all around the world. To illustrate, earlier this year, President Obama signed an Executive Order, "Promoting Private Sector Cybersecurity Information Sharing," focused on improving information sharing by encouraging the formation of information-sharing analysis organizations, with the goal of expediting the creation of trusted relationships to facilitate more robust information sharing. Additionally, multiple bills currently being considered in the U.S. Congress are intended to spur the voluntary sharing of cyber threat information among and between businesses and federal entities to improve cybersecurity, and all of these bills define cybersecurity threat information so as to include information related to vulnerabilities. The overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity. The onerous licensing scheme contemplated by the BIS Proposed Rule, however, would necessarily slow down the sharing of vulnerability information (both intra-company and between companies). In other words, because the Proposed Rule is effectively erecting additional barriers to vulnerability sharing, it appears diametrically opposed to the goals of multiple cybersecurity policy initiatives currently being advanced across the U.S. government.

Furthermore, we detail below how the BIS' Proposed Rule would significantly impact a potentially wide range of cybersecurity products and technologies in development, as well as restricting research into cyber vulnerabilities and exploits connected to valuable internal business activities, including intra-company transfers of vulnerabilities. Both of these sets of activities – whether developing innovative defensive cybersecurity products, or research into and testing to determine vulnerabilities in our core products and technologies (e.g., through Intel's Secure Development Lifecycle processes) - are intended to strengthen the cyber defenses worldwide of Intel and our customers. At a minimum, the licensing scheme envisioned by the Proposed Rule would negatively impact the ability of companies in the U.S. seeking to develop such products, and would almost certainly leave critical data systems much less protected and subject to increased cyberattacks or breaches by malicious actors, because of the inevitability of delays associated with applying for and receiving approvals for license applications.

3. Impact to Intel

At Intel, the Intel Security Group performs research using intrusion software to provide products that are able to secure the worlds' networks properly. Intel's chip security organization delivers open source framework tests made publicly available, with a proprietary version for internal use. Intel's live threat laboratories work on active rootkits and malware which is deeply essential research to test threat mitigation. Intel Security products such as Vulnerability Manager can perform intrusive checks, to identify weaknesses so that they can be remediated; they are not specifically designed for exploitation. To be able to detect and remediate vulnerabilities, Intel must retain the ability to identify and test those vulnerabilities. Even products that are not "specially designed" to perform this

¹ The Cyber Threat Alliance is a group of cyber security practitioners from organizations that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member organizations and their customers. <http://cyberthreatalliance.org/>

² Page 1-2; https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

single intrusion function may be captured under the breadth of the Proposed Rule as written. Intel's Product Security Incident Response Team is dedicated to preempting malicious attacks, but the language of the Proposed Rule does not preclude such proactive security testing from export controls with sufficient clarity. If there is no technical difference defined in the EAR between the cybersecurity activities performed by Intel and the criminal activities performed by "hackers", Intel will be significantly hampered by the imposed controls. Intel would then be unable to collaborate with industry partners to resolve security issues and threats in real time due to the licensing requirement.

A. Chilling Effect on Security Research and Collaboration

Leveraging the open source/publicly available exemption from the EAR, security companies may choose not to publish or otherwise make publicly available information concerning security vulnerabilities or the techniques they are using to safeguard their own and their customers' products and networks. Nevertheless, Intel needs to share information about such vulnerabilities and techniques among its foreign subsidiaries, foreign national employees, and even with other companies and entities facing similar issues in order to continuously protect and troubleshoot products. Information-sharing within the security community working for protection and mitigation must be freely authorized under the final rule. Implementing targeted end use and end user controls via EAR Part 744, rather than broadly applicable (NS1, RS1, AT) country controls on 4D001, 4D004, 4E001, 5D002, and 5E002 software and technology subject to this rule would more accurately restrict exports for criminal/malicious end users and limit the negative impact to Intel's internal security and vulnerability operations. The creation of a targeted narrow end use and end user based control would enable BIS to more effectively distinguish malicious or "black hat" hackers while not controlling the methods and tools necessary for developing cybersecurity capabilities.

B. Burden of Deemed Exports and Intra-Company Technology Transfer Licensing

Using Intel's own Information Technology business group as a case study, out of 6,059 active employees worldwide, 48.5% (2,942) are non-U.S., non-Canadian, foreign or third country nationals who would require individual or "broad" export authorizations to permit uninterrupted security and threat assessment work should the Proposed Rule be published as written with NS, RS, and AT controls imposed. Immediately requiring export licenses for continued use of hardware and software tools for cybersecurity activities associated with internal product design and validation would cause a work stoppage in nearly half of Intel's worldwide IT operations. BIS will need licensing officers prepared to receive, process, and issue to Intel:

- a. 115 individual deemed export licenses for foreign nationals in IT in the U.S. alone;
- b. 140 individual deemed export licenses for third country nationals; and
- c. 16 site-wide export licenses for Argentina, Brazil, Chile, China, Costa Rica, India, Israel, Korea, Malaysia, Mexico, Poland, Romania, Russia, Singapore, and Taiwan.

Intel would need to immediately disrupt worldwide operations to accommodate the addition of new ECCNs for cybersecurity software and associated technology to facilitate continuous worldwide business operations. Scaled to the size of Intel's entire employee population of 111,817 individuals worldwide, the deemed foreign national licensing burden increases by a factor of eighteen—an overwhelming operational demand on Intel, BIS, and reviewing agencies, contrary to the intended goal of the Proposed Rule and Export Control Reform to ease licensing for exporters and the U.S. government alike.

C. Potential Abuse of Open Source and Publicly Available Exemption

BIS' FAQ on the Proposed Rule explicitly excludes open source products; Intel's goal in cybersecurity research is to enable the world to use the Internet in a safe, enriching way, and our research and development efforts require continued ability to make security software tools open source and/or publicly available as a public service for the worldwide cybersecurity community. To contrast, closed source tools performing the same functionality would fall under export controls if the Proposed Rule is published as final, including Core Security Core-Impact, which features detection evasion from anti-malware, Canvas, Cobalt Strike, and similar. Software manufacturers could elect to make all tools open source to avoid undue

export control in the proposed cybersecurity rule, thereby bypassing the intention of the rule and exposing users of intrusion software to information security vulnerabilities. For Intel, the use of tools for internal research and development activities would be restricted from any non-U.S. or Canadian nationals. If an export license were required to authorize use of such components and software, Intel's ability to perform security testing, vulnerability analysis, and ensure its products are generally safe for public use would be severely constrained.

D. Delayed Remediation for Security Vulnerabilities

The urgent need for collaboration is particularly acute when there is an ongoing attack. The vague intent to make available some form of "broad export licenses" will not provide Intel the compliance tools (due to likely onerous license conditions) to conduct research on and discovery of previously unknown threats on an increasingly frequent basis. Intel notes that network security professionals responding to attacks simply do not have the luxury of debating the fine distinctions of whether a particular element of technology or software may be classified under ECCN 4D001, 4D004, 4E001, 5D002, 5E002, or EAR99. Neither can Intel or other companies debate the merits about whether it might need to be added to a "broad license" contemplated by BIS before sharing it throughout their network operations centers and taking necessary defensive actions across their worldwide networks.

Without a clear licensing or license exception structure such as ENC(a)(1) for internal design/development in place in advance of the publication of the final rule, industry work on 4D004 and 4D005 software will completely cease while companies scramble to apply for individual deemed licenses. Specifying controls based on **end use** rather than subjecting the software and technology to comprehensive license requirements would mitigate this internal collateral damage, as Intel's scope of activity in cybersecurity exists within design and development for the security of its own products and customers

E. Disruptive Presumptive Denial Policy

Even more alarming, BIS' proposal would advance "a policy of presumptive denial" for zero day and rootkit capabilities, e.g., "product or system" or "delivery tool" (p. 28855). Presumptive denial would greatly restrict Intel's ability to share threat information and counter some of the most dangerous cyber vulnerabilities and exploits, as well as efforts of companies to share information internally and with peers in the industry in order to counter critical cyber vulnerabilities and exploits.

4. Recommendations

As a result of the complexity of the technical and policy issues raised by the Proposed Rule, Intel Corporation strongly recommends BIS, along with its inter-agency partners, to withhold the Proposed Rule from publication.

In lieu of non-implementation, Intel Corporation advises that BIS limit the scope and coverage of the Proposed Rule as a narrower definition is required to avoid disrupting day-to-day business operations. Specifically, Intel recommends that BIS address the use of systems, equipment, components and software "specially designed" for launching attacks by identifying the technical parameters that distinguish malicious attacks from non-malicious attacks/testing. A vehicle to help address the absence of technical differentiations could be a working group of technical experts representing industry and government focused on the variance between "defensive" and "offensive" cybersecurity measures. The working group would be able to provide BIS with information that can be utilized in a focused and narrow end use and end user based control which differentiates between "white hat" developers who are seeking to improve security across the eco-systems and "black hat" hackers who are focused on substantially harming an information system or data on an information system. This in turn will enable BIS to set appropriate export controls based on malicious end use which do not inadvertently subject Intel and others to burdensome and onerous internal licensing requirements in order to conduct day-to-day business.

If Intel's recommendation for end-use/end-user based control cannot be accommodated, at a minimum Intel BIS establish a self-executing license exception mechanism under §740 of the Export Administration Regulations (EAR)

that does not include reporting requirements. The license exception should be structured to enable exporters to export, re-export, and transfer (including in-country transactions) systems, equipment, components, technology, and/or software for internal company use worldwide.

Intel appreciates the opportunity to comment on the Proposed Rule and looks forward to continuing its cooperation with the U.S. Government on export control reform.

Best Regards,

Jeff Rittener

Jeff Rittener
Senior Director, Global Trade
Intel Corporation

Cc.
Mario R. Palacios, Director, Import and Export Policy

PUBLIC SUBMISSION

As of: July 27, 2015
Received: July 27, 2015
Status: Posted
Posted: July 27, 2015
Tracking No. 1jz-8k7u-9qfq
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0214

CompTIACommentsDOCWass2013ProposedRuleFinalClean

Submitter Information

General Comment

See attached

Attachments

CompTIACommentsDOCWass2013ProposedRuleFinalClean



July 20, 2015

Sent via email to: publiccomments@bis.doc.gov

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Subject: RIN 0694-AG49

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Sir or Madam:

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry. With approximately 2,000 member companies, 3,000 academic and training partners and nearly 2 million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

Thank you for the opportunity to provide comments on this rule which proposes to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013 with regard to systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor. BIS proposes a license requirement for the export, reexport, or transfer (in-country) of these cybersecurity items to all destinations, except Canada. Although these cybersecurity capabilities were not previously designated for export control, many of these items have been controlled for their "information security" functionality, including encryption

and cryptanalysis. This rule continues applicable Encryption Items (EI) registration and review requirements, while setting forth proposed license review policies and special submission requirements to address the new cybersecurity controls, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items. BIS also proposes to add the definition of "intrusion software" to the definition section of the EAR pursuant to the WA 2013 agreements.

Through this rule BIS is proposing new export control requirements for systems that communicate with "intrusion software", which could place unprecedented restrictions on how companies, researchers and governments can share and receive security threat information from their non-U.S. employees, other companies, academic researchers, and users. The impact on the security of products and services globally could be catastrophic, slowing down patching and updating to glacial speeds.

U.S. companies have a long history of exchanging security-related information with their users (bug reports), university researchers (security vulnerabilities), information with their own employees (threat analysis), etc. This real-time feedback helps companies protect their systems from intrusions and provide the best security possible for billions of users of Internet services, software, and mobile apps, through the provision of quick patches and updates. In February 2015, President Obama issued an [Executive Order](#), stating that "private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible" and encouraged the creation of new information sharing analysis organizations to improve security. Given the importance of these sharing efforts, [the Department of Commerce announced](#) last week that it would be kicking off a voluntary, multi stakeholder process in September to help foster the disclosure of vulnerability information to improve computing security.

Under the [WA](#), 41 governments have voluntarily agreed to maintain a common set of national export control lists through domestic legislation and regulation. These lists include items such as military equipment, weapons of mass destruction (WMD's), as well as dual-use items such as software and technology normally used for civilian purposes but which may have military applications.

Under a new 2013 definition, the sending of any material/code relating to a system that communicates with "intrusion software" beyond a WA member state's borders, must be export-controlled by each member state. The EU implemented this definition across its member states in January 2015 and companies and security researchers are already being required to get export licenses first before sharing threat or vulnerability information tied to "intrusion software" with U.S. entities - including companies, academics, nonprofits, and governmental organizations (like US-CERT). This has resulted in significant confusion.

Through this rule, BIS is seeking to implement these export control requirements in the Export Administration Regulations (EAR) — which is expected to not only impose similar export conditions in the U.S. but validate the use and implementation of this WA definition in other countries. BIS released a preliminary [FAQ](#) attempting to clarify the influx of concerns they've received so far, but the FAQ addresses only a handful of concerns expressed by companies relating to the definition, specifically carving out exploit samples, malware, and proof of concepts, while continuing to control legitimate platforms and defensive systems that companies use to defend against intrusion software delivery mechanisms.

This rule proposes to amend Section 772.1 by adding the following term “Intrusion software” and associated definition:

§ 772.1 Definitions of terms as used in the Export Administration Regulations (EAR).

Intrusion software. (Cat 4) “Software” “specially designed” or modified to avoid detection by `monitoring tools,' or to defeat `protective countermeasures,' of a computer or network-capable device, and performing any of the following:

(a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; *or*

(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes: 1. “Intrusion software” does not include any of the following:

a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;

b. Digital Rights Management (DRM) “software”; or

c. “Software” designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

2. Network-capable devices include mobile devices and smart meters.

Technical Notes: 1. `Monitoring tools': “software” or hardware devices, that monitor system behaviors or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

2. `Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

BIS has not yet clarified why this “intrusion software” definition is being proposed for inclusion in U.S. regulations in the first place, since WA is a purely voluntarily agreement focused on national security controls, while this definition focuses instead on addressing criminal activities. Secondly, BIS has not clarified why the current iteration of the definition has to be implemented by the U.S. government, instead of pushing for a proposal to modify the definition at the December 2015 WA Plenary, prior to any implementation in the U.S. Thirdly, the proposed BIS rule does not discuss how BIS’s use of broad license exceptions have already been implemented in the Code of Federal Regulations to protect legitimate business and individual uses of technology, and how that could be applied in this instance for legitimate security purposes.

CompTIA has the following comments on the sections of the proposed rule and the specific questions directed to industry:

BIS is seeking information about the effect of this rule and would appreciate the submission of comments, and especially answers to the following questions:

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:

a. The number of new licenses that U.S. companies would have to request could range from those in the single digits to numbers in the thousands, depending on the number of products in their individual portfolios, the volume of third-party software and services they use in their own operations, the number of offices they have outside of the U.S. and Canada, and the number of non-U.S. national security engineers working in the U.S. under a nonimmigrant visa who are employed by or in contact with each company. In addition, the burden of determining what needs a license would be significant for the standard software development cycle, such as:

- i. Information in issue tracking systems.
- ii. Comments in code.
- iii. Code in transient states that may meet this definition ephemerally.
- iv. Email communication containing information that this regulation would control.

To the extent that BIS maintains a restrictive policy with respect to “rootkits” and “zero-day exploits,” it should provide clearer definitions of what types of items are included, particularly with respect to distinguishing between malicious software and information and patches that are intended to identify potential vulnerabilities and prevent malicious intrusions.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

a. Yes, “intrusion software” as defined in WA, and proposed for implementation by BIS, would severely restrict security vulnerability improvements and research for U.S. companies, academia, nonprofits, and individuals - given that it covers not only entities creation or operation of intrusion software, but also any system that “communicates with” such software. The proposed export control, via the definition of “intrusion software” from WA, would impose severe limitations on:

- i. The sharing of information between a single company’s employees or computers - across borders - or even across the same room, if someone within the US shares technical data about security threats with someone who is not a national of the US or Canada.
- ii. The sharing of threat information between companies.
- iii. The development, operation, and functionality of automated security vulnerability identification and reporting tools, API’s, or backend systems that companies build into their own products to defend their systems.
- iv. The speed of deployment of security patches for products impacted by intrusion software or related exploits (e.g., POODLE).
- v. Vendors that companies use for security/threat intelligence.
- vi. E-mail accounts set up by companies to specifically receive security threat and vulnerability information from the general public.
- vii. Products that companies sell to provide threat intelligence functionality.
- viii. The work of security vulnerability researchers at U.S. and international universities, who currently share threat information directly with U.S. companies (e.g., zero-day vulnerabilities) over e-mail.
- ix. Bug bounties and Hackathon events, which are created to specifically identify security exploits and then share that information back with the affected companies as quickly as possible.
- x. The information that companies or researchers can share across security and threat sharing partnerships (e.g., Sector Coordinating Councils, Information Sharing and Analysis Organizations).
- xi. The information that can be shared with the U.S. government voluntarily (e.g., US-CERT) or as required under procurement contracts (e.g., FISMA, FedRAMP). In addition, currently proposed legislation in the United States for sharing cyber

threat information with the federal government could be significantly impacted and undermine the process and liability protections afforded to U.S. companies.

- xii. The types of audits that companies would be allowed to perform on third-party vendors systems and whether bugs could be reported back to them directly when found.

CompTIA member companies recommend that BIS forestall the implementation of these rules, and revisit their scope with WA partners, as it seems clear that what appears to be the original intent of these controls – to limit the activities of illegitimate organizations and malicious hackers – has been exceeded, and is far more likely to impose significant burdens on legitimate businesses and security professionals who are trying to defend themselves from such bad actors.

Our member companies do not dispute that some sort of controls are appropriate on the export of truly malicious items. A “catch and release” system, where overly broad ECCNs “catch” not just the tools used by malicious hackers, but also the tools used to defend against their cyberattacks, and the “release” is a burdensome individual licensing scheme that will be used only by the “good guys,” is unlikely to have any negative impact on the “bad guys” and may even make it easier for them by reducing industry’s ability to react to cyberattacks.

If the United States and its Wassenaar partners are having difficulty distinguishing between items that are used defensively vs. offensively, we encourage greater interaction with the manufacturers and users of such equipment to develop ECCNs that exclude items used for defensive purposes, while maintaining controls on the export of malware. An avenue for government to gain a better understanding of the potential impacts of the proposed rule would be for BIS to engage directly with industry and establish a working group composed of technical experts from government and industry to systematically address the technology differences between offensive and defensive cybersecurity items. More rational, targeted controls will also harmonize these export control efforts more closely with the President’s encouragement of industry to share vulnerability information, rather than working at cross purposes with it. CompTIA member companies believe that adjusting the scope of controlled ECCNs is the best approach, as our WA allies do not uniformly use License Exceptions in their national implementation of multilaterally agreed controls.

In parallel, CompTIA member companies encourage BIS to consider implementation of more flexible License Exceptions and licensing policies to authorize legitimate exports of controlled hardware, software, and technology, as has been done with respect to items subject to EI controls. The current proposal excludes many items from License Exception eligibility.

CompTIA member companies encourage the development of License Exception eligibility for cybersecurity items that would authorize:

1. Release of controlled items to a company's own employees and contractors, as well as to other companies headquartered in the United States or other WA countries for internal use;
2. Release of vulnerability information to manufacturers of vulnerable items and their agents for purposes of vulnerability remediation, as well as exchange of information between manufacturers and entities who have identified such vulnerabilities to them;
3. Release of vulnerability remediation software and information to end-users of vulnerable products;
4. Release of vulnerability information to governments, organizations, and companies headquartered in the United States and other WA countries for the purpose of providing preventative and remedial information about cybersecurity vulnerabilities.

Implementing such a License Exception would likely reduce the burden on industry significantly, without undermining the goal of denying controlled items to bad actors. Both industry and government would benefit, as we doubt there are resources available to process what could be a crushing number of individual licenses involving deemed exports, intra-company transfers, and transfers between and among affiliates of companies headquartered in the United States and WA countries.

We also encourage the US Government to encourage its Wassenaar partners to implement parallel exceptions and policies, to enhance the ability of legitimate users of these items to work collaboratively to defeat cyberthreats on a worldwide basis.

Similarly, adopting more flexible licensing schemes for cases where License Exceptions would not apply, such as allowing transfers of unlimited quantities of such items to trusted strategic partners and end-users, as is done with Encryption Licensing Arrangements, would be a better alternative to the individual license process and familiar to the regulated industry from the encryption controls.

We doubt the rationalization of the scope of controls, or the adoption of appropriate License Exception eligibility and more flexible licensing policies, would have a negative impact on national security or cybersecurity, but rather would have the opposite effect of supporting government and industry objectives of sharing information between legitimate users to support immediate defensive reactions to cyberthreats. We encourage the US Government to explore both paths as a means of reducing the negative impact of these proposed rules.

Finally, we note that many items that would be subject to the proposed new ECCNs are currently subject to control under Category 5, Part 2, and the proposal indicates that certain requirements of EAR parts 740.17 and 742.15 will continue to apply to such items, even though they will be subject to control under ECCNs Category 4 or Category 5, Part 1. This will likely cause confusion, particularly because exporters will already have received CCATS covering many such items. While the proposal includes notes in the new ECCNs advising exporters that certain encryption-related requirements are a pre-requisite to a license, and there is a proposed note to 5A002 that indicates the primacy of the cybersecurity ECCNs, there is a possibility that some exporters will feel caught in an infinite loop and get confused.

We suggest that BIS include clear guidelines in the regulations, in FAQs, and in flowchart form clearly delineating the order of review for cybersecurity items, and clearly stating the prior classification, reporting, and ERN registration requirements are applicable to cybersecurity items that also contain encryption functionality.

The language in proposed 748.3(z) is a clearer statement of the parallel encryption-related requirements, as opposed to the notes to proposed ECCNs, which state, with minor variations:

License Requirement Note: *All license applications for [ECCN] must include the information required in Supplement No. 2 to part 748 of this EAR, paragraph (z). Also, all such cybersecurity items using or incorporating encryption or other “information security” functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, must also satisfy the registration, review and reporting requirements set forth in §§ 740.17, 742.15(b) and 748.3(d) of the EAR, including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD prior to applying for a license.*

The last sentence of this note could be confusing, as it implies that all 4D004 items with the specified encryption functionality are subject to a mandatory encryption review and Supplement 6 submission requirement. It is possible that some such items may be authorized for Mass Market under 742.15(b)(1) or ENC under 740.17(b)(1) or other sub-paragraphs that do not require submission of a CCATS or Supplement 6. We recommend that the note either omit that “including submissions to the ENC Encryption Request Coordinator, Ft. Meade, MD,” and just state that exporters must comply with the cited sections, or else add the phrase, “to the extent required” to the end of the sentence.

Thank you once again for the opportunity to provide comments on this proposed rule.

Sincerely,



Ken Montgomery
Vice President, International Trade Regulation & Compliance

PUBLIC SUBMISSION

As of: 7/28/15 10:50 AM
Received: July 28, 2015
Status: Posted
Posted: July 28, 2015
Tracking No. 1jz-8k8e-81gk
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0215

RIN 0694-AG49 SIA Comments on Cybersecurity

Submitter Information

General Comment

See Attached

Attachments

RIN 0694-AG49 SIA Comments on Cybersecurity

July 20, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Room 2099B
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Ave., N.W.
Washington, D.C. 20230

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation:
Intrusion and Surveillance Items (*Federal Register* Notice of May 20,
2015; RIN 0694-AG49)

Dear Ms. Hess:

The Semiconductor Industry Association (“SIA”) is the premier trade association representing the U.S. semiconductor industry. Founded in 1977 by five microelectronics pioneers, SIA unites over 60 companies that account for nearly 90 percent of American semiconductor production. The semiconductor industry accounts for a sizeable portion of U.S. exports.

SIA is pleased to submit the following public comments in response to the request for public comments issued by the Commerce Department’s Bureau of Industry and Security (“BIS”) on proposed revisions to the Export Administration Regulations (“EAR”) pertaining to intrusion and surveillance items.¹

I. The Proposed Interpretation of “Intrusion Software” Inappropriately Fails to Exclude Software for Defensive Activities

The interpretation of “intrusion software” put forward by BIS is overly broad and all-encompassing and fails to make any distinction between software employed for malicious, offensive activities on the one hand and software employed for purely defensive, protective activities on the other.² The Proposed Rule would control systems, equipment, components (4A005) and software (4D004) that are specially designed or modified for the generation, operation, or delivery of, or communication with, “intrusion software”. The Proposed Rule also would control technology (4E001.a) if required for 4A005, 4D004.a (if required for 4A005 or 4D004) and if required for 4E001.c. The manner in which software meeting the characteristics of “intrusion software” is employed directly implicates the impact of the software on cybersecurity and so should play a central role in determining the export controls associated with the software.

¹ Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015) (“Cybersecurity Proposal”).

² Cybersecurity Proposal at 28,858.

BIS has indicated that:

some penetration testing products marketed as defensive products meet the technical description of such command and delivery platforms in the new control list entries. . . . **It is BIS's understanding that there is no technical basis to distinguish defensive products from offensive products (i.e., a defensive product may be used offensively).**³

BIS has failed to establish that there is in fact no technical basis on which to distinguish defensive products from offensive products. Such distinctions are possible and more work is needed to identify technical distinctions.

A vehicle to help address the absence of technical differentiators could be a working group of technical experts representing both industry and government. The task of this working group would be to identify the technical differences between “defensive” and “offensive” cybersecurity measures. For example, the working group could provide BIS with technical details pertaining to technology and software that destroys, renders unusable, or substantially harms an information system or data on an information system which in turn will enable BIS to set appropriate controls that do not inadvertently subject exporters to burdensome and onerous licensing requirements in order to conduct day-to-day business. Distinguishing between offensive and defensive activities will enable BIS to set appropriate controls that do not inadvertently subject SIA members to onerous and unnecessary licensing requirements.

Operational or use distinctions between offensive and defensive activities are readily available and can effectively separate cybersecurity activities that pose national security risks from those that do not. Indeed, such distinctions are made in several pieces of legislation pending in the U.S. Congress. The Cybersecurity Information Sharing Act of 2015 (S.754) would permit private entities to monitor, and operate defensive measures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on their own information systems and allow entities to share and receive indicators and defensive measures with other entities or the federal government. The legislation defines a “defensive measure” to be:

an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability . . . {exclusive of a} measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to -- (i) the private entity operating the measure; or (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.⁴

The Protecting Cyber Networks Act (H.R. 1560), which passed the House of Representatives on April 22, 2015 by a vote of 307-116, and the National Cybersecurity Protection Advancement

³ Intrusion and Surveillance Items FAQs, available at <https://www.bis.doc.gov/index.php/licensing/embassy-faq#subcat200> (emphasis added).

⁴ S.754, Section 5.

Act of 2015 (H.R. 1731), which passed the House on April 23, 2015 by a vote of 355-63, both also utilize the term “defensive measure.”

Similar distinctions should be utilized by BIS so that software employed for defensive measures are not controlled as “intrusion software.” Companies today perform vulnerability assessment using software that may fall within the proposed interpretation of “intrusion software,” but should not be controlled as it is employed for purely defensive activities -- for example, the delivery of open source framework tests involving work on active rootkits and malware that is essential research to test threat mitigation. In addition, commercially available IT system vulnerability software products can perform intrusive checks, but are not specially designed for exploitation. To be able to detect and remediate vulnerabilities, companies must have the ability to exercise such software.

SIA members also may use third parties for penetration testing who use other software meeting the proposed interpretation of "intrusion software," and for purposes of testing, those third parties may use such software against their locations outside the US. This type of "white hat" vulnerability scanning or testing should not be impeded by these restrictions.

I. Certain “Intrusion Software” Should Not Be Subject to Control

All software meeting the broad parameters of “intrusion software” is captured by the proposed interpretation, regardless of the type or character of software or its availability. Mass-market software and open source software should not be subject to additional export controls even if they meet certain parameters associated with “intrusion software.” Indeed, SIA understands that the Wassenaar Group discussions held in 2013 had not intended to treat mass-market software or open source software as cybersecurity software warranting stringent export control.

The interpretation of the term “intrusion software” should be narrowed to include only software that is proprietary, not generally available, and specially designed for offensive activities. Legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using “intrusion software” should not be included. Accordingly, ECCN 4D004 should not include general purpose network penetration testing products.

The majority of current security research and development (“R&D”) projects are cross-border, international efforts leveraging resources in countries across the world to provide robust and timely analysis and remediation. Such R&D efforts would be hampered significantly if software employed for defensive activities are not excluded from the interpretation of “intrusion software,” meaning that the ability of SIA member companies to perform security testing and vulnerability analysis would be severely constrained.

II. If the Interpretation of “Intrusion Software” is Not Narrowed and Appropriate Exclusions Provided, A New License Exception Should Be Created to Cover Non-Threatening Exports of Such Software

If BIS chooses to maintain the proposed interpretation of “intrusion software,” BIS should modify EAR section 740 to include a new self-executing license exception (License

Exception “CYB”) pertaining to hardware, software and technology falling within ECCNs 4A005, 4D004 and 4E001 used in a particular manner.

Specifically, the following types of exports of items within ECCNs 4A005, 4D004 and 4E001 should be included within the new license exception:

1. Intra-company transfers

Companies frequently maintain information technology (“IT”) staff in several different countries and seamless interaction between those IT staff is required for efficient operation of the company. Intra-company transfers of intrusion and surveillance items and technology pertain only to the defense of corporate networks and so should not be subject to licensing requirements. Exports and deemed exports of “intrusion software” items should enjoy exemption from controls similar to those applying to intra-company transfers of encryption items set forth in License Exception ENC [Section 740.17(a)(2) of the EAR].

2. Exchange of Security Vulnerability Information

Many companies choose not to publish or otherwise make publicly available information concerning security vulnerabilities or the techniques they are using to safeguard their own and their customers’ products and networks. Nevertheless, they need to share information with respect to such vulnerabilities and techniques between and among their foreign subsidiaries, foreign national employees, and even with other companies and entities facing similar issues. Indeed, Executive Order 13,691 articulates such an information sharing requirement. The urgent need for this kind of collaboration is particularly acute where there is an ongoing attack.

3. Exports to be Used for Purely Defensive Activities

As indicated above, it is possible to distinguish between “defensive measures” and “offensive measures.” Any export associated exclusively with the former actually enhances, rather than harms, cybersecurity and so should not be of concern to the U.S. government. Any such export should not be licensable.⁵

In order to avoid a massive escalation of license applications and/or a counter-productive reduction in defensive cybersecurity measures implemented by U.S. companies, BIS should, at a minimum, create a new license exception covering such exports.

Without the ability to transfer and use these tools freely at their worldwide sites, SIA member companies may have to apply to BIS for thousands of export licenses just to support

⁵ There are several examples within the EAR of use-based exceptions. Among those are (1) Regional Stability (RS) controls apply to Microwave “Monolithic Integrated Circuits” (MMIC) power amplifiers in 3A001.b.2 and discrete microwave transistors in 3A001.b.3, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications; (2) 3A001.a.2 does not apply to integrated circuits for civil automobile or railway train applications; (3) the inclusion of human rights considerations in licensing policy within EAR Part 742; and (4) end use and end user prohibitions within EAR Part 744.

daily security and vulnerability analysis activities. This would result in thousands of work hours for BIS and exporters, work stoppages worldwide, and increased security threats for customers while exporters wait for license processing.

III. Conclusion

As drafted, the proposed interpretation of “intrusion software” is overly-broad and imposes license requirements that are unnecessarily restrictive, significantly increasing compliance burdens on SIA members. If either that interpretation is not revised or the licensing requirements are not modified, SIA members may be required to obtain a large number of additional export licenses for products and services that are used for overwhelmingly legitimate purposes.

Moreover, if implemented as drafted, the proposed rule would impede the ability of SIA members to protect their own networks and their customers’ data – undermining cybersecurity rather than enhancing it. To gain a better understanding of the potential impacts of the proposed rule, BIS should engage directly with industry and establish a working group composed of technical experts from government and industry to systematically address the technology differences between offensive and defensive cybersecurity items.

At a minimum, if BIS chooses to maintain the proposed interpretation of “intrusion software,” BIS should modify EAR section 740 to include a new self-executing license exception (License Exception “CYB”) pertaining to hardware, software and technology falling within ECCNs 4A005, 4D004 and 4E001 used in a particular manner.

The Proposed Rule implicates complex technical and policy issues. SIA urges BIS to pause its current push to issue a final rule, and instead, to take the additional time needed to fundamentally reconsider the proper approach to these controls. Among other steps, BIS should convene technical workshops for input and insight from industry and the security community. After such fact-gathering, BIS should issue a new proposed rule that focuses on a narrower set of items and avoids imposing undue compliance burdens on legitimate cybersecurity efforts.

* * * * *

SIA appreciates the opportunity to comment on the Proposed Revisions and looks forward to continuing its cooperation with the U.S. Government on export control reform. Please feel free to contact the undersigned or Joe Pasetti, Director of Government Affairs at SIA, if you have questions regarding these comments.



Cynthia Johnson
Co-Chair, SIA Export Control Committee



Mario R. Palacios
Co-Chair, SIA Export Control Committee

PUBLIC SUBMISSION

As of: 7/29/15 2:55 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-eo51
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0216

Jonathan Brossard Toucan System

Submitter Information

General Comment

See attached

Attachments

Jonathan Brossard Toucan System

Sharron Cook

From: Jonathan Brossard <jonathan.brossard@toucan-system.com>
Sent: Wednesday, July 22, 2015 5:58 AM
To: PublicComments
Subject: Feedback on Wassenaar Arrangement 2013 Plenary Agreements Implementation

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Dear Federal Rulemaking Portal team,

I am a well known security researcher, and happen to be the Principal Engineer of Product Security at Salesforce.com .

I am writing you in regards to the proposed Wassenaar Arrangement. While I do certainly agree that a portion of intrusion software - such as the ones recently leaked from hacked Italian company HackingTeam - are a threat to our businesses, and the internet at large, I would like to express my concerns in regards to the prohibition of proof of concepts exploits and automated vulnerability scanners : I use those on a daily basis to make Salesforce.com and ultimately a significant share of our top businesses' marketing data more secure. Our task in keeping our data safe is already tremendously hard : I am affraid that the new proposed regulation might make our task even harder and give an edge to attackers (who do not care so much about the legality of their actions).

Thanks and regards,

- - -

Jonathan Brossard
Founder/Chief Executive Officer
<https://www.moabi.com>
<http://twitter.com/endrazine>

Toucan system
PO BOX 330143
San Francisco, CA
94133

Toucan System SARL,
8 Allée Saint Thomas,
63400 Chamalières
FRANCE

Toucan System Pty Ltd
PO BOX Q1355
Queen Victoria Building
Sydney NSW 1230
AUSTRALIA

PGP Key ID: 0x463DDEFE

<http://www.toucan-system.com>

<http://twitter.com/#!/toucansystem>

This email may contain information which is confidential and is intended only for use of the recipient/s named above. If you are not an intended recipient, you are hereby notified that any copying, distribution, disclosure, reliance upon or other use of the contents of this email/fax is strictly prohibited. If you have received this email in error, please notify the sender and destroy this email.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2.0.22 (GNU/Linux)

iEYEARECAAYFAIWvaUMACgkQSR1YzUY93v6YXACgvzqZ+an4KWiE871dg7tPEh4b
AH4AnRggDkzID2HtM8dtniZtPabLO3Wc
=VBlj

-----END PGP SIGNATURE-----

PUBLIC SUBMISSION

As of: 7/29/15 2:59 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-temw
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0217

Technet Mike Ward 7-29

Submitter Information

General Comment

See attached

Attachments

Technet Mike Ward 7-29

July 17, 2015

Kevin Wolf
Assistant Secretary of Commerce for Export Administration
U.S. Department of Commerce
Washington, D.C. 20230

Hillary Hess
Director, Regulatory Policy Division
U.S. Department of Commerce
Washington, D.C. 20230

Catherine Wheeler
Director, Information Technology Controls Division
U.S. Department of Commerce
Washington, D.C. 20230

**Re: Comments on Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)**

Dear Assistant Secretary Wolf, Director Hess, and Director Wheeler:

On behalf of TechNet, the nation's premier network of innovation economy CEOs and senior executives, I write to express our deep concern with the proposed rule, by the Commerce Department, Bureau of Industry and Security ("BIS") in the *Federal Register* on May 20, 2015 (the "Proposed Rule").

While the proposed rule was developed in an effort to address companies that create or sell "weaponized software" used to breach information technology systems, the rule as submitted for comment will impact businesses and practices far beyond "weaponized software" companies. Therefore, while this rule may have been a well-intentioned effort to protect national security interests and preserve human rights, the significant damage it will inflict on the cybersecurity must be considered.

In particular, TechNet believes that the Commerce Department should reconsider this proposed rule because of the damage the current draft will do to the cybersecurity industry in the following ways:

- The proposed rule will dramatically restrict U.S. companies' access to legitimate cybersecurity tools through onerous restrictions on the export of both cybersecurity technologies and testing tools, even when those tools are only exported to foreign subsidiaries of U.S. companies.

- The proposed rule will also negatively impact research into cybersecurity vulnerabilities as researchers would be hindered from testing networks and sharing technical information across borders.
- The proposed rule also creates significant risks to intellectual property rights by potentially requiring companies to provide source code and other intellectual property to the United States Government.
- Finally, tri-directional collaboration on cybersecurity risks, a longstanding priority of the United States Government, would be harmed both within cybersecurity companies and among customers and industry partners, as information deemed “exported” if shared with non-U.S. persons, even if physically located in the U.S.

TechNet and its members appreciate the extremely complex set of issues surrounding this topic and would welcome the opportunity to further engage with the BIS and any other department or agency in an effort to find a satisfactory answer to this vexing topic.

Sincerely,

Mike Ward
Vice President, Federal Policy and Government Relations
TechNet

PUBLIC SUBMISSION

As of: 7/29/15 3:01 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-27xj
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0218

Red Hat Amy Ross 7-29

Submitter Information

General Comment

See attached

Attachments

Red Hat Amy Ross 7-29

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49) Published in 80 Fed Reg 28853 on May 20, 2015

Dear Sir/Madam:

On behalf of Red Hat, Inc., we appreciate the opportunity to submit these comments on the above referenced matter. As we explain below, the Proposed Rule is over broad, poses a major burden on industry with potentially significant unintended consequences and may not achieve the intended purpose of the Proposed Rule. We strongly recommend that the Bureau of Industry Security (BIS) postpone the Proposed Rule's implementation and significantly narrow its scope.

Red Hat is the world's leading provider of open source software solutions, delivering reliable and high-performing cloud, Linux, middleware, storage. An S&P 500 index member, Red Hat provides high-quality, secure and affordable technology solutions that are found throughout mission-critical systems in the financial, transportation, telecommunications and government sectors and in enterprises in the United States and around the world. Red Hat is recognized as one of the world's most innovative companies.¹

The Proposed Rule includes several issues of concern to Red Hat, in particular, the interpretive issue found in the Supplementary Information section of the Proposed Rule at page 28854 under the sub-heading, Scope of the New Entries. It reads in relevant part:

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.

In order to achieve what we understand is the intended purpose of the Proposed Rule, we strongly suggest that the scope of control on intrusion items should be strictly limited to platforms for launching attacks and technology required for the development of those platforms. Examples include platforms developed and marketed by companies like FinFisher and HackingTeam.

1 See <http://www.forbes.com/innovative-companies/list/>. See, also, Forbes, "The World's Most Innovative Companies", Sept. 2012, found at: <http://www.forbes.com/innovative-companies/list/>.



The limited, publicly available information on these and similar companies suggests that FinFisher's FinSpy and HackingTeam's Remote Control System (RCS), respectively, are suites of equipment, software and services used for surveillance and monitoring. In both suites, there is a specific application that acts as the administrative command center, listing and managing the recovered information. According to reports, FinFisher also offers a hardware platform with pre-loaded software for the operation and delivery of intrusion software.

On the other hand, legitimate network penetration testing products and technologies, which may have been developed in in the process of defending against attacks perpetrated using Intrusion Software, should be outside the scope of this Proposed Rule. Among the network penetration testing programs that are widely used are those produced by companies are Metasploit and Nessus.

Both of these exemplary products are available in versions that qualify for decontrol either under (a) the Wassenaar General Software Note, as they are publicly available; and/or (b) the Wassenaar Cryptography Note , because they are mass market. Hence, other Wassenaar member countries would not control either of these software programs. However, with regard to Metasploit, for example, the Proposed Rule appears likely to control one element (Metasploit Pro, which is mass market) but not another (Metasploit Framework, which is publicly available).

Therefore, it is especially important that BIS not interpret ECCN 4D004 in a manner that would implement controls on general purpose network penetration testing products. Based on the information available to us, it appears that the relevant authorities of Japan implementing its export control policies have reached agreement with its affected domestic industry to avoid such an interpretation. To include general purpose network penetration testing products would not achieve the purposes of the Proposed Rule, and would be detrimental to other objectives outlined by the Administration regarding enhancing cybersecurity.

Finally, we respectfully submit that security vulnerability technology, software and related services should be excluded from the scope of the EAR when shared with the intent to defend against possible attacks. Alternatively, BIS should consider the creation of a license exception authorizing the export of security vulnerability technology, software and related services, without pre-export review or post-export reporting requirements to cover technical exchanges intra- and inter-company.

For these reasons, Red Hat respectfully requests that BIS postpone its implementation of the Proposed Rule so that these issues can be directly addressed in an updated draft for comment of the Proposed Rule.

Again, we appreciate the opportunity to comment on this matter. Please do not hesitate to contact us if you have any questions, or if we can provide additional information.

Sincerely,

A handwritten signature in blue ink that reads "Amy B. Ross".

Amy B. Ross
Manager, Export Compliance

A handwritten signature in black ink that reads "Mark Bohannon".

Mark Bohannon
Vice President, Global Public Policy

PUBLIC SUBMISSION

As of: 7/29/15 3:03 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-ecws
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0219

Privacy International BIS submission 7-29

Submitter Information

General Comment

See attached

Attachments

Privacy International BIS submission 7-29

Background

This comment is submitted by Privacy International in response to the proposed rule (RIN 0694-AG49) implementing controls on intrusion and surveillance items agreed within the Wassenaar Arrangement in 2013.

Privacy International, a registered UK charity (No. 1147471), was founded in 1990 and was the first organisation to campaign at an international level on privacy issues. Privacy International ("PI") envisions a world in which the right to privacy is protected, respected, and fulfilled. Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.

Part of the work that Privacy International does is to investigate the secret world of government surveillance and expose the companies enabling it. We raise awareness about technologies and laws that place privacy at risk, to ensure that the public is informed and engaged.

Throughout our history we have proactively engaged with and rigorously campaigned on issues relating to export restrictions. Throughout the 1990s, when governments were trying to restrict individuals' access to encryption, together with the wider privacy community, we fought against such restrictions, highlighting the threat that such measures pose to individual privacy and the security of our modern technological infrastructure.

More recently, we have campaigned for export restrictions to apply to surveillance technologies which represent a fundamental risk to privacy and a range of other human rights. PI coordinates a global coalition aimed at ensuring surveillance technologies are not used to facilitate human rights abuses or internal repression. The Campaign Against Unlawful Surveillance Exports brings together human rights, arms control, tech policy, and media freedom civil society groups to campaign for stronger safeguards to prevent the use of surveillance technologies in ways that undermine fundamental human rights.

We therefore welcome initiatives aimed at achieving greater oversight of the trade in surveillance technologies, including the 2013 agreement at the plenary of the Wassenaar Arrangement (WA) to include IP Network Surveillance Systems and items related to intrusion software on the dual use control list. Since then, we have been closely monitoring the implementation of the controls by participating states.

It is evident that export control policy and international cooperation on export controls stems historically from strategic state decision-making related to national security and foreign policy interests. The core criteria for including an item within control lists include the ability to make a clear and objective specification of the item. This objective specification becomes increasingly difficult where technology underpinning surveillance equipment is similar, and in some cases the same, as that used within commercial and civilian applications and techniques. While this is a common issue within dual use export regulation, the potential for regulations within the computer and telecommunications network security context to have negative consequences upon individuals and IT security research makes regulatory measures within this field particularly challenging and vitally important to get right in a clear and concise manner.

Nevertheless, if export regulations and international cooperation in export policy are to remain a relevant mechanism for fostering human rights and international security, it is essential that they are updated to take into account new technologies while protecting security research and the free flow of information. We believe that the inclusion of these items into the WA control list was done in good faith because of these reasons. Their inclusion represents a positive recognition that the unregulated sale of surveillance technologies by security vendors constitutes a risk to individual human rights and security.

The proposed rule has, however, caused widespread and serious concern among many sectors because of the potential inherent in it for unintended consequences, particularly the potential of language used within the new the proposed controls on items related to intrusion software to affect security research and the overall security of the internet. This is a concern that PI shares and we also recognise that there are limitations in respect of what the WA control list can achieve. Efforts to protect individual privacy, other human rights, and the security of modern networks, devices, and applications in the modern technological environment rely upon security research and international cooperation amongst researchers. Additionally, many of the technologies that may at first instance seem to be offensive in nature actually serve a vital component in building effective defensive capabilities for us all. The imposition of export licensing requirements therefore must only be upon strategically chosen, well-defined surveillance technologies, with explicit protections and exceptions for research.

It is our view that the US export control regulatory system and BIS's implementation of the items related to intrusion software require further clarification and safeguards. We strongly recommend that in order to fulfill the initial objectives of the controls an approach which takes into account the intent of the technology and software developer and by

incorporating end-use and end-user controls, and exceptions upon specific items. In addition, we recommend updating the WA dual use list language itself to clarify and provide certainty for all security researchers in the 41 states that adhere to the controls.

Given the need for further consultation, it is essential that another proposed final rule is published with clarifications and that another opportunity for public comment is provided, before a final rule is promulgated.

The remainder of this submission comprises the following sections:

- 1. Why effective controls are a necessary and effective step**
- 2. The proposed control of IP Network Surveillance Systems**
- 3. The proposed control of items related to intrusion software**

1. Why effective controls are a necessary and effective step

The human rights impacts of surveillance exports are becoming increasingly evident: the private text messages of activists are read out to them as they are tortured; mass surveillance technology appears on the market, for purchase by repressive regimes that wish to monitor, collect and store the communications of entire populations; political refugees find their computers have been hacked and their digital life stolen. Surveillance technologies are used by governments to target opponents, journalists and lawyers, crack down on dissent, harass human rights defenders, intimidate populations, discourage whistle-blowers, chill expression and destroy the possibility of private life. In some cases, they also used to subject entire populations to indiscriminate monitoring. In short, they are often part of a broader state apparatus of oppression, facilitating a wide variety of human rights violations including unlawful interrogation practices, torture and extrajudicial executions.

The most obvious right affected by surveillance technology is the right to privacy, as any interception with communications or collection of personal data constitutes an interference with the right to privacy. Other rights that are frequently directly affected by surveillance include the right to freedom of expression and the right to freedom of association.

While subjecting specific surveillance technologies to export restrictions is not a silver bullet designed to comprehensively protect human rights, it is a necessary and major component of a comprehensive approach to ensuring that such items are not used for abuses and that states who assist in such abuses are exposed. Any strategy must also include the adoption of effective legal frameworks and systems of oversight within states using surveillance technologies, the widespread availability and adoption of encryption and anonymization technologies, and access to secure networks, devices, and applications. Importantly, even when they are not invoked to restrict a transfer of surveillance technology, export controls also act as an essential accountability and transparency mechanism.

It is therefore necessary and welcome that the new items were included within the 2013 WA control list. The WA also requires its members to regulate transfers of other surveillance technologies, such as mobile phone interception equipment known in the US as Stingrays, and laser microphones used to eavesdrop on conversations, for example through glass windows. It is important for the WA participating states to ensure that its control lists are up to date and appropriately control all surveillance technologies the trade of which represents a threat to the enjoyment of human rights.

While human rights are not considered a motivational factor for the decision to regulate the technology within Wassenaar, it is clear that the two states which instigated the inclusion of the new categories into the regime; France and the United Kingdom; were motivated at least in part by concerns relating to human rights.

2. The proposed control of IP Network Surveillance Systems

The category relating to IP Network Surveillance Systems in the WA was initiated by France after evidence emerged that a French company, Amesys, supplied internet backbone monitoring technology to Gaddafi's Libya. The Wall Street Journal reports that Amesys' Eagle monitoring system – a combination of probes using Deep Packet Inspection technology and analysis software – was “deployed against dissidents, human-rights campaigners, journalists or everyday enemies of the state” in Libya.¹ Amesys is facing an ongoing criminal case into its complicity in acts of torture by the Gaddafi regime.²

¹Wall Street Journal, “Life Under the Gaze of Gadhafi's Spies” (14 December 2011), available at <http://online.wsj.com/news/articles/SB10001424052970203764804577056230832805896>.

²Business & Human Rights Resource Centre, “Amesys lawsuit (re Libya),” available at <http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496>.

The IP Network Surveillance control goes a considerable way in subjecting many of the most prominent internet monitoring centers available on the market to control, including that of Amesys's product Eagle. As of 1 January 2015, the EU Dual-Use Regulation 429/ 2008 restricts the export of specialised large-scale IP monitoring systems, such as that sold by Amesys. France implemented the control almost immediately after it was approved by the WA in 2013.

i) Concerns

The requirement that the system must perform all of the listed functions, however, including relationship mapping, significantly narrows the range of products affected by the regulations. Carrying out analysis on “carrier class IP network” is aimed at targeting powerful analysis systems – specifically those that have the capacity to carry out large-scale analysis reliably. What constitutes “carrier class” is, however, open to interpretation, while there are a number of definitions that could be cited by competent bodies. “Analysis at the application layer” also greatly restricts the scope of the control, given that many surveillance products operate at layers other than the application layer.

Extraction of selected data and its indexing means that the product under restrictions needs to be actively retrieving the metadata and content from the IP traffic as well as actively storing this data.

Further, the controls call for the product to be “specially designed” to search through the captured data based on certain characteristics of an individual (such as name, political affiliation, etc) and must use be able to collate the captured data to identify relationships between the targeted individual or group.

ii) Recommendations

Privacy International believes that it is important that non-IP monitoring centres are also included within the WA control list, and recommends that the US government review export restrictions over such IP and non IP turnkey surveillance systems and brings them within national and WA control lists.

Regarding the implementation of ECCN 5A001j, we welcome the decision to designate the items as controlled for reasons of Regional Stability, which will mean that the items are assessed on a case-by-case basis and that promoting the observance of human rights will be a criteria used to assess applications. We strongly recommend that human rights implications are prioritised within the assessment process and that assessment criteria also includes:

- The compliance of the destination country with human rights obligations enshrined in the Charter of Fundamental Rights, the International Covenant on Civil and Political Rights, and other ratified instruments;
- The human rights record of the beneficial end-user authority, namely the agency or body proposing to purchase the technology, and;
- The existence or absence of an appropriate legal framework governing the use of the technology in the destination country, sufficient to ensure that the technology will be used in a manner compliant with human rights.

3. The proposed control of items related to intrusion software

The addition of items related to intrusion software were proposed by the United Kingdom and also agreed at the WA in December 2013. The following is a selection of PI's previous public comments on the topic:

- Announcement of controls on intrusion software and IP surveillance: <https://privacyinternational.org/?q=node/398>
- Export controls and implications for security research: <https://privacyinternational.org/?q=node/354>
- Open source software and export controls: <https://www.privacyinternational.org/?q=node/344>
- Our previous analysis of the US proposed rule: <https://www.privacyinternational.org/?q=node/588>

The targets of these additions to the dual-use list are items that have been popularly referred to by media as “state trojans”, “lawful malware”, or “spyware”. They are marketed by security vendors for exclusive use by law enforcement and intelligence agencies as primarily useful for extracting data from a network-enabled device and for taking remote control of the device in order to actively monitor an individual target. The UK government has stated that these controls were targeted at “complex surveillance tools which enable unauthorised access to computer systems.”³

The controls distinguished between components used to create and control the surveillance software and the software itself. For instance, such technology works by installing a Trojan on to networked devices and then using it to control functions such as the microphone or transmit data to a monitoring facility. The WA control does not target the Trojan component, but rather the command and control infrastructure used to generate, install and instruct the Trojan – i.e., the

3 https://www.techuk.org/images/CGP_Docs/Assessing_Cyber_Security_Export_Risks_website_FINAL_3.pdf

software installed on a government controlled server to deliver the Trojan to a target address. UK authorities have stated that this delineation was put in place to protect security researchers (i.e., those participating in sharing malware samples) and individuals infected by Trojans, given that any control on the Trojans themselves would put individuals carrying them on devices across borders under potential breaches of export regulations.

Subjecting such systems to export restrictions is necessary to protect human rights. The intrusive nature of this type of monitoring and intelligence gathering, the fact that it can be used against targets located anywhere in the world, and the absence of a clear and robust legislative framework governing their use makes these unlawful in their use. Widely-available evidence in the public domain shows how such products have been sold by companies and subsequently used for human rights violations.

High profile vendors of the targeted items based in the European Union, which implemented the controls within the Dual Use Regulation at the beginning of 2015, have indicated that their national export authorities have implemented the category into national law and are seeking export authorisation for their export.

Earlier this month, internal documents relating to Hacking Team, an Italian surveillance company, were leaked online. The documents showed that the company has customers listed in some 45 countries, including Azerbaijan, Bahrain, Colombia, Egypt, Ethiopia, Kazakhstan, Morocco, Oman, Russia, Saudi Arabia, Sudan, Turkey, UAE, and Uzbekistan. Hacking Team have a distributor in the US, Cicom, and have sold their technology to various US customers, including the Army, Federal Bureau of Investigations, and the Drug Enforcement Agency. The documents also show that Hacking Team was not subject to export restrictions before the implementation of the new controls, and that they believe that they are now subject to individual license authorisation to export to countries outside of the WA.

Privacy International believes that this underlines both the necessity of subjecting the export of such systems to restrictions and license assessment criteria which prioritize human rights obligations.

i) Concerns

PI agrees with many of the general concerns already publicly advanced and submitted via this public comment process. In order to protect individual privacy and other human rights, and the security of the devices, networks and applications relied upon by everyone, including journalists, activists, and political opposition in authoritarian states, it is essential that implementation of the controls does not restrict security research. Subjecting specific security research tools and activities to restrictions, reporting requirements, and deemed exports provisions risks undermining the protection of privacy, as well as the commercial, foreign, and other interests of the US.

Privacy International's understanding from correspondence with the UK export control licensing authority was that the WA control was structured in a way to protect security research. These categories are not primarily intended to restrict exports of software vulnerability exploits, Proof of Concepts for such exploits, vulnerability research and non-public reporting of software vulnerabilities, training and international cooperation on how to identify and exploit vulnerabilities, commercial penetration testing software tools, fuzzers, or the presentation of research at international security conferences.

Privacy International believes that many of the above activities and items may not be subject to regulation by the proposed rule because they are either not defined within the scope of controls, because they are exempted as fundamental research, because they are ordinarily made publicly available, or because they are not "technology". Nevertheless, we appreciate that the definitions of controlled items may subject critical security research activities and security research tools to regulation and impede or chill research activities that help protect network infrastructure and personal privacy interests.

For example, category 4e001c, technology required for the development of intrusion software, requires greater clarity and more effective implementation. This category would control exploit "technology", defined as technical data (blue prints, design plans) or technical assistance (training), if it is for the "development" of software "specially designed" to avoid protective measures (anti-virus software) and extract or modify data or modifying the standard execution path of software in order to allow the execution of externally provided instructions, and if the export is not subject to a "publicly available technology and software" exception. The fact that a controlled item needs to be "technology" "required" for the "development" of intrusion software and that software needs to be "specially designed" and "peculiarly responsible" to fulfill all of the functions considerably narrows the scope of products subject to licensing. The proposed rule would not control technology simply for discovering or identifying vulnerabilities, or testing the vulnerability to determine what happens. We also acknowledge the realities of many security processes such that much of the research conducted will never become publicly available and therefore, the publicly available exception is not adequate.

This would mean, however, that if an individual were to, for example, draw up a design plan of how to develop an

exploit “specially designed” to carry out of these functions, and were to “export” it to a foreign company or to a non-US national, then they would require a license. This has implications for individuals and companies involved in research cooperation. Given the publicly available exception and protections for fundamental research, this would primarily affect independent researchers and those in the private sector who need to be able to collaborate, often across borders or with non-US nationals. Employees within the same company would not be exempted under the current language. Often, security researchers are not affiliated with an academic institution, and have no control over whether such “technology” is ever made publicly available. Indeed, in some cases, it is undesirable for the “technology” to be made publicly available, given that it is then made available for attack. It also has implications for companies involved in specialised training. If a company was providing training for profit on how to develop that particular type of exploit, they would need a license. They would also need one for training non-US individuals.

The control on the “software,” “systems,” “equipment,” or “components” “specially designed” for the generation, operation or delivery of, or communication with, “intrusion software” will regulate some essential security research equipment. For example, commercial penetration testing tools that are not open source and that are considered “specially designed”, require a license for export.

To a large extent this is because of the decision in the proposed rule not to implement the first paragraph of the Wassenaar Software Note. Although the open source exception applies, the “mass market” exception – anything generally available to the public through normal points of sale – does not apply to any of the categories. We understand that the basis for this decision is that most items identified as potentially controlled were already controlled because of the controlled encrypted functionality within them and were therefore already not eligible for exemption. However, this is extremely problematic. UK authorities noted to Privacy International that the WA General Software provides additional protections for the security research community, because they believed that software targeted at the penetration testing community is almost exclusively open source or commercially available without restriction and thus not subject to this export control because of the General Software Note (GSN). While the GSN provides essential protections however, it is not sufficient to take into account the realities of how security research is conducted and accordingly we are calling for additional safeguards to be expressly stated in the text of any regulation.

Some security research tools will not be subjected to restrictions because they are not considered to be “specially designed” to carry out the functions in the controlled categories. Nevertheless, as a notoriously complex area of export control law to understand, this will chill security research and the development of security tools by small and medium enterprises and individuals not familiar with export regulations, even if they are not in fact subject to any restrictions. It is vital that any regulation be clearly and concisely stated in writing and in the actual text of the regulation itself – Privacy International does not consider any FAQs or telephone calls to be sufficiently authoritative in respect of this issue.

Deemed Exports regulations will further amplify the negative consequences of implementing the proposed rule in its current form. While there are exceptions protecting research and the dissemination of research at public conferences, this will most obviously have negative implications for research cooperation, training on use of controlled security research tools, and the provision of specialised training on how to develop “intrusion software” to customers abroad or to non-US citizens in the US.

ii) Recommendations

All of the categories related to intrusion software require greater clarity and more effective implementation. Privacy International recommends that additional exceptions be applied to the categories and that specific activities and items are clearly excluded from control in any final rule. As a result of the confusion and concerns caused by the new categories, we also strongly recommend that a new proposed final rule is published and that another round of public comments is made available.

We recommend that additional exclusions are included to narrow the scope of the new licensing requirements to only apply if the exporter is aware that the export may be intended for ultimate end-use by a government end-user for the monitoring of IP network enabled-devices for intelligence gathering or law enforcement purposes. While this approach suffers from enforcement difficulties, it is nevertheless still an effective means by virtue of the fact that the vast majority of surveillance technology manufacturers explicitly and exclusively sell their products to government end-users for the purposes of surveillance. We also recommend that additional exclusions are put in place to consider the purpose and motivation for the work. For example, it would not be appropriate to restrict a researcher sending a PoC to a government agency regarding a vulnerability in its website or other software system.

A precedent for this approach exists within the CIV exception. For example, for certain items on the CCL list that usually require a license for export to the ultimate destination, the CIV exception allows items to be exported to civil-end users for civil end-uses in selected countries. This license exception is available if the item is controlled only for national security (NS) reasons. Such an exception applied to the categories related to intrusion software would therefore

only regulate the export of “technology” or systems if they are intended to be used for surveillance by government end-users, and would avoid placing regulatory burdens upon security research not intended to be used in that area.

Further exceptions should also be applied in order to clarify what activities and items are explicitly not subject to restrictions to stop the chilling effect of any complex regulations. We recommend that any security research items and activities subject to restrictions that BIS is aware of and that have been brought to its attention via this public comment process be explicitly excluded from licensing requirements within the rule itself, even if they are already excluded by the general exceptions or are not subject to restrictions in the first place. Such items and activities include, but are not limited to, software vulnerability exploits, Proof of Concepts for such exploits, vulnerability research and non-public reporting of software vulnerabilities, training and international cooperation on how to identify and exploit vulnerabilities, commercial penetration testing software tools, fuzzers, and the presentation of research at international security conferences. The research on any of these must also be protected, whether it is publicly available or not.

A precedent for this approach exists within the APP exception. This exception enables exports of computers and associated technology and software of certain “Adjusted Peak Performance” (APP) levels to certain groups of countries, provided there is no evidence of intention for certain end uses. Such an exception can be used in relation to the new categories to explicitly exclude specific technology from control.

We also recommend that the mass-market exception within the GSN be reinstated.

We welcome the decision to designate the items related to intrusion software as controlled for reasons of Regional Stability, which will mean that the items are assessed on a case-by-case basis and that promoting the observance of human rights will be a criteria used to assess applications. We strongly recommend that human rights implications are prioritised within the assessment process and that assessment criteria also includes:

- The compliance of the destination country with human rights obligations enshrined in the Charter of Fundamental Rights, the International Covenant on Civil and Political Rights, and other ratified instruments;
- The human rights record of the beneficial end-user authority, namely the agency or body proposing to purchase the technology, and;
- The existence or absence of an appropriate legal framework governing the use of the technology in the destination country, sufficient to ensure that the technology will be used in a manner compliant with human rights.

Privacy International thanks BIS for their attention in this matter and is available for further consultation on any of the issues discussed above.

PUBLIC SUBMISSION

As of: 7/29/15 3:05 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-qekk
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0220

Palo Alto Networks Ryan Gillis 7-29

Submitter Information

General Comment

See attached

Attachments

Palo Alto Networks Ryan Gillis 7-29

Palo Alto Networks Comment Regarding: “Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Reform.”
(Docket ID: BIS-215-0011; RIN 0694-AG49)

Palo Alto Networks appreciates the efforts by the U.S. government to solicit widespread input regarding the implications of the proposed rule regarding the “Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Reform.” We also appreciate the underlying goal of this agreement, which is to keep cyber attack tool sets out of the hands of people, organizations and states with malicious intentions.

However, we are concerned that export controls are not an effective means to accomplish this laudable goal, and the unintended consequences of implementing this agreement – particularly as envisioned under the proposed rule – could result in an overall decrease in cybersecurity and network defense efforts.

Our concerns are broader than any potential direct implication for new export controls on our current products. Companies that produce cybersecurity products, and operators charged with protecting networks, benefit from complementary defensive technologies and techniques developed not only by companies and nations, but also through formal and informal groups and individuals around the globe. This necessary work often occurs across national boundaries – including through the collaboration of employees for multinational companies, and unstructured relationships with individuals. Applying export controls to these entities and critical activities will, at a minimum, disadvantage legitimate networks defenders and vendors who are under attack.

Software attack tools, unlike typical products regulated under export controls, can literally be built by anybody who has a laptop, a compiler, and a mindset that is keen to understand how things work and how one might subvert an original design for other purposes. Additionally, attackers do not have to start from scratch. The basic designs of Stuxnet, Flame and DuQu are readily available on the Internet. It would not take much for a small team of modestly resourced hackers to build their own attack platform. Furthermore, buying exploits to feed their attack platform would not be difficult. The underground economy for exploits has flourished with the development of the Internet. These new export rules will not affect that in the least.

Equally important, malicious attackers and legitimate network defenders routinely use the same technologies and techniques for very different purposes. Security companies, software developers, and white hat hackers often run intrusion software in order to test existing protective measures, discover vulnerabilities, and remediate those issues. It is common practice that this intrusion software must also be shared along with the underlying infrastructure that the proposed rule and official FAQs attempt to distinguish and treat separately:

[T]he proposed rule would not control any “intrusion software,” which may also be referred to as malware or exploits. The Category 4 control entries would control the command and delivery platforms for generating, operating,

delivering, and communicating with “intrusion software.” It would also control the technology for developing “intrusion software,” but it does not control the “intrusion software” itself. Thus, transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware would not be included in the new control list entries and would not require a license under the proposed rule.¹

Functionally, this distinction is difficult, if not impossible, to implement when identifying and remediating these issues, and preventing the “intrusion software” from being successful. At best, requiring legitimate actors to attempt to do so provides an additional advantage to the malicious attackers.

The proposed rule also includes “a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.”² While speed is essential in identifying, protecting against, and remediating “zero-day exploit capabilities,” it seems inevitable that well-intentioned entities would be prevented from sharing, or mired in export control procedures before sharing, the information and technology necessary to close these vulnerabilities.

Again, Palo Alto Networks appreciates this opportunity to comment on this proposed rule, and hopes to continue the dialogue on this issue.

¹ www.bis.doc.gov/index.php/policy-guidance/faqs.

² www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

PUBLIC SUBMISSION

As of: 7/29/15 3:06 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-t4jf
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0221

OEI Tech FINAL Jim Ramsbotham 7-29

Submitter Information

General Comment

See attached

Attachments

OEI Tech FINAL Jim Ramsbotham 7-29

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
US Department of Commerce
14th Street and Pennsylvania Avenue, NW
Washington, DC 20230

(Submitted by e-mail on 20 July 2015)

Subject: Comments on Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694–AG49)

Dear Sir/Madam:

I appreciate the opportunity to comment on this rule. After careful review I believe that, as written, the language strictly interpreted has a number of potentially draconian unintended consequences. I would respectfully submit that these need to be addressed before the four questions posed under Request for Comments can be reasonably answered.

The crux of the problem is this:

The phrase “specially designed” is not a defined term in the Wassenaar. There, by common practice, I believe the English usage of undefined terms as defined in the Oxford English Dictionary is used. This allows for the application of judgement and common sense in the practical interpretation of the meaning in context.

By contrast a strict reading of the language of the term as implemented in US Export Controls does not appear to allow any latitude when applied to “Systems and equipment” in 4A005. This same lack of latitude will extend to technology controls in 4E001.

The proposed language for 4A005 reads as follows:

4A005 “Systems,” “equipment,” or “components” therefor, “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”.

Substituting the language of the definition for “specially designed” results in the following text

4A005 “Systems,” “equipment,” or “components” therefor, ~~“specially designed”~~ having “as a result of “development” ~~has~~ properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions of, or modified for the generation, operation or delivery of, or communication with, “intrusion software”.

The exceptions defined in subparagraph (b) of the definition of “specially designed” apply only to listed types of products. Commodities not listed, including “Systems and equipment” are excluded.

The problem becomes potentially acute when the control specifications are broad functional capabilities and the logic of the control language is inclusive—which is the effect of the use of “or” in 4A005. For BIS’s consideration:

- From the amount of concern, effort, and resources being devoted to cybersecurity, I submit that “intrusion software” having the characteristics specified in the definition control language exists, and that, as for other software products, their sellers describe a minimum configuration required for their use.
- If this minimum configuration specifies performance or any attribute of a decontrolled computer, a strict interpretation of the language of “specially-designed” will by definition catch that computer, and any system or equipment meeting or exceeding the specifications.
- Under these conditions, if the development goals and specifications for such a computer had to be laid against the stated minimum hardware requirements for using the “intrusion software” the exporter has no practical basis for claiming that it is exempt from export control.

There is no apparent escape clause for commodities, other than those specified in (2) of the definition of “specially designed”.¹ The exclusion clauses in (b) do not apply to “systems and equipment.” Thus, I believe that strict application of the inclusive the language creates will catch the product if, it has any of the attributes specified.

To compete in the global economy, US industry needs clear, unambiguous, legally-binding regulatory language—language that can be referenced and applied equitably in a court of law. Recognizing the difficulties of harmonizing and rationalizing export controls across the board, I would respectfully suggest that, as a minimum, BIS consider making the intent of the regulations clear by crafting an exception note along the following lines.

4A005 does not apply to systems and equipment designed or sold for computing applications other than for the use of intrusion software. Systems and equipment designed for general-purpose use, or specially-designed for other uses (e.g., for military use), must be evaluated against the relevant provisions of the CCL and USML to determine their export-control status.

These comments have been narrowly focused on the proposed language of 4A005. They do not address the effect of RS controls to all countries except Canada in 4E001. In the absence of a clear “escape clause” for “specially designed” items not categorized in (2) of the definition of “specially-designed” similar unintended consequences are likely in other parts of the EAR and ITAR controls.

The effect of the ITAR is outside the scope of this announcement. However, I am of the strong opinion that until the combined effects of export control reform taking both EAR and ITAR are fully understood and language modified to reflect the actual intent of the government, the practical effects of either are going to be difficult if not impossible to assess. To pick one specific, I note the clarification of the intent in an announcement related to the use of specially designed in the Munitions List. That language attempts to deal with the problem of an escape clause for commodities in paragraph (a)(1), with the following statement:

So, even if a commodity or software is capable of use with a defense article, it is not captured by paragraph (a)(1) unless someone did something during the commodity’s development for it to achieve or exceed the performance levels, characteristics, or functions described in a referenced USML paragraph.

I imagine myself an exporter in a court of law, charged with exporting a product that has one or more of the performance characteristics or functions described in a reference USML category. How do I make the case that no one did anything in any aspect of development to give my product the performance levels, characteristics, or functions it actually has. I respectfully implore the government to consider the dire implications of such a situation for US industry, and to undertake to revise the regulations to ameliorate them to the extent possible.²

Thank you for taking the time to consider these comments,

Sincerely



Alan J. Ramsbotham, Jr.
King George, Virginia.

¹ This is not to assert that there may not be an escape clause elsewhere in the EAR Export Control Reform, of necessity, has been developed and implemented in parts. The complexity, volume, and extensive cross-referencing has made effective review an egregious challenge, and I, personally have not been able to find one. (For example, the Wassenaar Arrangement definition or “intrusion software”, critical to understanding the scope of the proposed language, is not provided in the subject Federal Register announcement.)

² One suggestion is that consideration be given to reviving a concept from the “anciene regime” (the COCOM). This was the understanding that “accidents of definition”—situations where strict interpretation would result in unintended consequences—would occur and would need to be addressed. The current environment is more complex in terms of number of players. However, the concept still may have validity and value, and may serve both exporters and enforcement well in the long run.

PUBLIC SUBMISSION

As of: 7/29/15 3:09 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-iigs
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0222

Northrup Grumman Tom donovan 7-29

Submitter Information

General Comment

See attached

Attachments

Northrup Grumman Tom donovan 7-29

July 20, 2015

Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th St. and Pennsylvania Ave., N.W., Room 2099B
Washington, D.C. 20230

ATTN: Ms. Catherine Wheeler
Director, Information Technology Control Division

SUBJECT: RIN 0694-AG49 - Wassenaar Arrangement 2013 Plenary Agreement Implementation:
Intrusion and Surveillance Items

Dear Ms. Wheeler:

Northrop Grumman Corporation (“NGC”) wishes to thank the Department of Commerce for the opportunity to provide comments to the above proposed rule as we support the Department's implementation of Export Control Reform. In response, NGC provides the following comments:

DOC Request for Industry Comments:

How many additional license applications would your company be required to submit per year under the requirements of this proposed rule?

NGC’s Enterprise Shared Services sector is home to the Cyber Threat Assessment & Awareness (“CTA&A”) organization which is an internal organization dedicated to performing cyber security assessments of NGC’s internal information systems located in the U.S. and abroad. The CTA&A organization use software tools and techniques that are known or suspected to be employed by adversaries trying to exploit and obtain unauthorized access to NGC’s information systems. NGC believes some of the software tools used by the CTA&A organization may be classified under proposed ECCN 4D004 and require a license to be exported when testing occurs at overseas subsidiaries and affiliates. The number of licenses required to support these activities is estimated to be between five (5) and ten (10) per year, but may be less given BIS’s intent to issue broad license authorizations.

How many additional applications would be for products that are currently eligible for license exceptions?

Of those applications, NGC believes all would be for products currently eligible for license exception ENC. Many of the products utilized by the CTA&A organization are ECCNs 5D002/5A002 due to the encryption functionality.

How many additional applications would be for products that currently are classified EAR99?

None.

Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

While BIS has emphasized that broad license authorizations will be available for 'cybersecurity items', the lack of exceptions and time and expense involved in the classification and licensing of items may impede NGC's ability to protect its internal networks. The licensing requirements may also slow the ability of NGC's CTA&A team to respond to new and emerging threats due to constraints on what may be exported and licensing timelines.

How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

It is difficult to quantify the time burden associated with answering questions proposed in paragraph (z) to Supplement No. 2 to Part 748. Many of the products utilized are developed and supplied by ~~by~~ third parties. As such, NGC may not be able to provide the full information requested by paragraph (z).

Additional Comments

Lack of License Exceptions

Under the proposed rule BIS uses the concept of 'specially designed' to identify items classified under ECCNs 4A005, 4D004, 4D001.a and 5A001.j to impose licensing requirements on 'cybersecurity items'. Items meeting the broad 'catch' of paragraph (a)(2), which describes "parts," "components," or "software" used in or with commodities... 'enumerated' or otherwise described on the [CCL] are therefore subject to stringent controls and ineligible for the vast majority of license exceptions. NGC believes that it will be difficult to apply the release criteria found in paragraph (b) to hardware and software obtained from third party vendors, as much of the information required to make accurate release decisions may not be available to the exporter.

NGC suggests that a license exception be available for 'cybersecurity items' similar to license exception ENC as described in 15 C.F.R. § 740.17(a)(2). Such an exception would authorize exports and reexports of systems, equipment, commodities, components and software classified under ECCNs 4A005, 4D004, 4D001.a and 5A001.j to any "U.S. subsidiary," wherever located, except in Country Groups D:1 and E:1. This would allow companies to protect and defend internal networks from malicious attack without the need for a license and would not contravene the policy objectives of the proposed rule.

Definition of 'Rootkit' and 'Zero-day Attack'

In the proposed rules BIS states there is a 'presumption of denial' for items that have or support rootkit or zero-day exploit capabilities. BIS also requires exporters to provide information on 'intrusion software' license applications to describe how rootkit or zero-day exploit functionality is precluded in accordance with Supplement No. 2 to 15 C.F.R. § 748(z). Without further details, we believe the use of these terms causes confusion and misunderstanding. Therefore, we suggest BIS add definitions for 'Rootkit' and

'Zero-day Attack' in 15 C.F.R. § 772 in order to provide technically precise definitions to help exporters evaluate the potential exportability of cybersecurity items.

NGC would offer the following as potential definitions of the terms:

Zero-day attack-- is a 'software' that exploits a vulnerability that has not yet been disclosed to the public. These exploits include attacks against software that the vendor is either: (1) unaware of, (2) is aware of, but has chosen not to fix, or (3) is in the process of fixing, but has not yet released an advisory or updated software to the public.

Rootkit-- is a 'software' program surreptitiously loaded onto a network designed to hide processes, files or conditions created by an attacker from detection by system administrator. The rootkit's ability to evade detection and enable continued privileged access is what sets a rootkit apart from other software.

Should clarification or subsequent technical discussions be necessary, please contact either Ryan Gardiner at ryan.gardiner@ngc.com, (703-280-3919), or myself at thomas.p.donovan@ngc.com, (703-280-4045).

Sincerely,

Thomas P. Donovan
Director, Export Management
Global Trade Management

PUBLIC SUBMISSION

As of: 7/29/15 3:10 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-15ya
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0223

NAM Comments to BIS_WA2013_FINAL 7-29

Submitter Information

General Comment

See attached

Attachments

NAM Comments to BIS_WA2013_FINAL 7-29

Linda Dempsey

Vice President

International Economic Affairs

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230.

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)

Via e-mail: PublicComments@bis.doc.gov

The National Association of Manufacturers (NAM) welcomes the opportunity to comment on the proposed rule issued by the U.S. Department of Commerce to implement the agreements by the Wassenaar Arrangement (WA) reached at the Plenary meeting in December 2013 regarding cybersecurity items like intrusion software and network surveillance systems.

The NAM is the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states. Today's connected environment allows manufacturers of all sizes to increase their productivity, speed innovation and take their businesses global. Manufacturers are entrusted with vast amounts of data through their comprehensive and connected relationships with customers, vendors, suppliers and governments. They are responsible for securing the data, the networks on which the data run and the facilities and machinery they control at the highest priority level. Additionally, manufacturers are the owners, operators and builders of our nation's critical infrastructure. They manufacture and use the temperature controls regulating the grain silos that store our food supplies. They build and manage the systems operating the traffic signals that set the rules of the road. They build and run the energy plants that power our homes and businesses as well as the heavy machinery exploring oil and gas fields. Manufacturers make technology products ranging from nanoscale electronic devices to fighter jets. Manufacturers leverage technology to design, produce and deliver these products, and technology is also used to manage, monitor and secure key facilities and products, including trade secrets and patents.

The products, controls, systems, patents, trade secrets and all other tools that differentiate manufacturers in the United States from their competitors abroad are vital to continued innovation and global competitiveness. The technology that enables and helps drive this innovation in the online environment has also created a new vulnerability: exposure to cyber thieves that are constantly attempting to penetrate networks to steal valuable intellectual property. This illegal activity allows bad actors to replicate products and designs and disrupt business activity and critical infrastructure. Manufacturers know they need to secure their networks, their controls and their data. Companies are engaged in ongoing efforts to strengthen their information technology networks and protect their IP, investing in information technology assets and hiring cybersecurity experts. Highly skilled cybersecurity researchers perform research, attend hacker conferences, network with their peers and then provide manufacturers and program managers with the tools to counter vulnerabilities. So-called "zero day" exploits are developed to demonstrate a suspected vulnerability, and the results from these exploits are then used to target and perform testing that ensures the vulnerability is resolved.

Leading Innovation. Creating Opportunity. Pursuing Progress.

The Department's proposed rule would require a license for the export, reexport, or transfer (in-country) of certain cybersecurity items to all destinations, except Canada. The proposed rule also contains Encryption Items (EI) registration and review requirements, while setting forth proposed license review policies and special submission requirements to address the new cybersecurity controls, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items. The proposal also puts forth a new definition of "intrusion software" for the Export Administration Regulations (EAR), pursuant to the WA 2013 agreements.

The proposal touches on complex technical and policy issues, and the NAM urges the Commerce Department to take the necessary time to reconsider fully the proper approach to these controls. As an example, the Bureau of Industry & Security (BIS) could convene technical workshops for input and insight from industry and the security community. After gathering facts and insight through those discussions, we urge BIS to issue a new proposed rule that focuses on a narrower set of items and avoids imposing undue compliance burdens on legitimate cybersecurity efforts.

If implemented as currently drafted, the proposed rule would seriously impair the ability of manufacturers to identify and fix software and other security vulnerabilities, while requiring thousands of export licenses. As drafted, the proposed rule would require licenses for virtually all exports, reexports, and deemed exports of an overly broad set of controlled items. The projected number of activities and tools subject to licensing controls in the software and IT industries generally is expected to be staggering. The significant compliance burden would likely have an overall effect of actually diminishing security for individuals and enterprises because the sheer volume of activities covered under the proposed rule would impose unreasonable burdens on the processing capabilities of both manufacturers and BIS, rather than placing the resources and efforts on the areas that would best address concerns that BIS may have.

Moreover, the proposed rule would likely hamper the efforts of cybersecurity professionals to protect critical networks and infrastructure against malicious intrusion by imposing delays and restrictions on the use of the best available tools to maintain security.

Manufacturers create products that are used in the world's critical infrastructures, and it is vital that we continue to ensure that our products are as secure as possible. Part of a product's secure development lifecycle program is to perform various security assessments in order to discover vulnerabilities – whether those are product features that could be exploited or simply bugs in the programming that would enable an attacker to remotely control or configure a device. The proposed rule would unfortunately discourage companies from performing those security assessments efficiently and effectively.

Thank you for the opportunity to provide comments on the proposed rule to implement the WA 2013 agreements regarding cybersecurity items. Manufacturers remain committed to working with the Department of Commerce and other U.S. agencies to improve and streamline U.S. export control requirements that will promote U.S. economic, national security and foreign policy interests.

Thank you,



Linda Dempsey

PUBLIC SUBMISSION

As of: 7/29/15 3:12 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-aml5
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0224

Internet association Abigail Slater 7-29

Submitter Information

General Comment

See attached

Attachments

Internet association Abigail Slater 7-29



INTERNET ASSOCIATION COMMENTS ON BIS IMPLEMENTATION OF THE WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS ON INTRUSION AND SURVEILLANCE ITEMS

1. Introduction

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies and their global community of users.¹ It is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Network security is of paramount importance to our member companies. They work tirelessly to defend their networks and their users' data from unlawful intrusions. Public policies that undermine the ability of security researchers to protect networks – whether by design or by default – are therefore highly relevant and important to us.

The members of the Internet Association would like to thank the Bureau of Industry and Security (BIS) for providing an open comment period regarding proposed changes to the Export Administration Regulations (EAR) implementing the Wassenaar Arrangement 2013 Plenary Agreements Implementation on Intrusion and Surveillance Items. We applaud BIS officials for requesting input to better understand how companies approach security and how this rule may negatively impact those capabilities.

Implementation of the Wassenaar Arrangement in the intrusion software space is an important topic with a number of complex and potentially competing interests. The recent compromise at Hacking Team in Italy puts this complexity in stark focus. While Italy had implemented the provisions of the Wassenaar Arrangement in its export laws, a company in Italy was actively selling and supporting intrusion software to foreign governments in the exact way that the arrangement was designed to prevent.

It is clear to us that BIS is trying to put in place rules with the right intentions. However, after reviewing the proposed rules, the BIS frequently asked questions, and summaries of conference calls held by BIS, the Internet Association believes that the rules in their current form could have a negative impact on our ability to defend our networks from attackers.

Before describing our concerns with the proposed rules and our recommendations, it is important to provide some background on the various methods our member companies use to improve the security of our own systems. By describing our general approach to security, we believe we can help BIS develop a better understanding of a complex and highly specialized discipline.

¹ The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits and Zynga.



2. How Internet Association Members Assess Security

In the broadest sense, approaches for assessing security of systems can be placed in two categories: process-focused assessments and technology-focused assessments. Process-focused assessments evaluate the **implementation** of security controls and their supporting processes by determining if they are in place and operating effectively. These are often non-technical assessments against a recognized standard such as the Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (aka SOC2), International Organization for Standardization 27001/2, or various National Institute of Standard and Technology (NIST) frameworks. These assessments determine whether controls are operating as expected based on their design.

Technology-focused assessments evaluate the **effectiveness** of controls, often by simulating the same approach an attacker takes to break into a network or systems. These assessments can take a number of forms including, but not limited to:

- *Internal/external vulnerability scanning*: where a security practitioner uses automated tools to identify potential vulnerabilities based on non-intrusive signatures. These scans are generally focused at the infrastructure layer (e.g. the operating system and common network services such as web server software and database software).
- *Internal/external network penetration testing*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities and attempt to exploit them to gain unauthorized access. As with internal/external vulnerability scanning, these assessments are often focused at the infrastructure layer.
- *Application assessments*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in a specific application and attempts to exploit them to gain unauthorized access. These assessments are often used to evaluate security on custom-built applications.
- *Source code reviews*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in the source code of a specific application. As with application assessments, these assessments are often used to evaluate security on custom-built applications, generally in combination with a broader application assessment.
- *Red team/Blue team exercises*: These exercises are the most open-ended form of security assessment and they most closely simulate a real-world scenario. During these exercises, security practitioners (called the “red team”) use a combination of automated and manual tools to identify vulnerabilities across an entire environment and attempt to exploit them to gain unauthorized access. Meanwhile, other security practitioners (called the “blue team”) attempt to detect the red team, investigate their activities, remove them from the environment, and exfiltrate data from the network. Throughout these exercises, the red team may, under company policy, have legitimate and legal access to data relevant to the exercise that is needed to prove its success and/or to gain additional access.
- *Bug Bounties*: where a company pays independent security researchers from outside of the company to identify and report vulnerabilities in a system, allowing the company to crowdsource the identification of vulnerabilities. The researchers who report these vulnerabilities can be from anywhere in the world.



While different companies may use a different combination of these assessments, most companies recognize the value provided by each type of assessment and tailor their security programs around them.

3. How Security Software Tools Support Company Assessments

Security software tools play a critical role in helping make security assessments more effective by improving security practitioners' capabilities in a number of ways, including:

- *Automation and Speed:* Many companies, especially the members of the Internet Association, have large infrastructures including hundreds of thousands of servers and hundreds of network services. There is no way to perform assessments of these large infrastructures without the automation and speed that these tools provide. Manually evaluating the susceptibility of each service, on each server, for each potential vulnerability is impossible.
- *Scale:* While related to automation and speed, scaling is important to call out individually. These tools not only let companies scale to the size of their environments but also let companies scale their talent. Using effective security tools allows a company to make a practitioner more effective by having them cover a wider breadth of systems and services. Given the difficulty in hiring talented security practitioners, scaling the ones we have is critical to supporting security in large environments.
- *Proof and Validation:* Once a practitioner finds a potential vulnerability, they achieve the best results from their efforts when they are able to validate the real risk of the vulnerability, not just the perceived risk. There is a significant difference in impact when a practitioner is able to say “this is what I was able to do” as opposed to “this is what I **may** be able to do.” The best way to validate the real risk of the vulnerability is to exploit it.
- *Simulation:* As explained above under “Red team/Blue team exercises”, the maximum value a security practitioner can bring is through the simulation of a real world attack. “Software” “specially designed” or modified to avoid detection by “monitoring tools,” or to defeat “protective countermeasures” of a “computer or network-capable device” describes tools that attackers use every day. A practitioner cannot simulate a real attack without using these types of tools.

4. The Value of Information Sharing

In addition to conducting assessments, companies often share information about emerging threats. This allows all participating companies to benefit from the efforts of a single company and respond to these threats more quickly. This information sharing happens in a number of ways including through commercial platforms, email lists, conferences, forums, and open platforms such as ThreatExchange (<https://threatexchange.fb.com/>). The latter platform is hosted by Facebook, an Internet Association member, and is used by a number of other Internet Association members, including Coinbase, Etsy, Google, LinkedIn, Netflix, Pinterest, Salesforce, Twitter, Yahoo, and Yelp, with more companies in the process of onboarding. Often, the information we share includes exhaustive details of tools, techniques, and procedures (TTPs) that we have seen attackers use within our networks. Sharing this level of detail maximizes the value of these exchanges.

As information sharing among organizations has grown, the value of this information sharing has grown as well. Many companies now view this as an integral part of their ability to detect and respond to new



threats. In fact, the U.S. government has recognized the value of this sharing as well, with President Obama issuing Executive Order 13636, “Improving Critical Infrastructure Cybersecurity”. (See Section 4 of the Order, stating “It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.”)

While we have seen an expansion in information sharing, the industry still has a very long way to go. Most companies are not actively sharing information or have limited information sharing capabilities. In the coming years, it is critical that we focus on doing everything we can to encourage broader information sharing (subject to appropriate privacy protections) across the industry.

5. Concerns with the Proposed BIS Rules

In light of the ways in which Internet Association member companies assess their security and the value of the threat information they share, they have a number of concerns with the proposed BIS rules:

1. **There is no intra-company exception built into the proposed rules.** As a result, companies may run afoul of the rules simply by sharing software or tools that leverage exploits for testing and validation purposes within their own teams. For example, some items controlled under the proposed rules would no longer qualify for License Exception ENC, which allows for intra-company transfers.
2. **The proposed rules are broad, ambiguous, and open to interpretation.** The ongoing discussions and clarifications are evidence of how difficult the proposed rules are to understand in their current form. To date, the clarifications have addressed specific examples or identified use cases, and have not effectively refined the broader context or scope of the proposed rules.
3. **In areas where the proposed rules are clear, they create a significant regulatory burden.** Any organization that wants to develop tools that would be controlled under the proposed rules will need to implement new or updated export control processes, which will incur additional costs and increase time to market. In addition, the proposed rules create enormously complex hurdles for individual researchers who might otherwise be able to make a meaningful impact on overall security.
4. **The proposed rules would have a chilling effect on information sharing and collaboration.** Companies and researchers might elect not to share information, even if permitted by the proposed rules, due to the difficulty in understanding their restrictions. This chilling effect will be felt most strongly by independent researchers or small security companies who may lack the resources or legal support to understand and comply with the proposed rules. The ambiguity of the proposed rules only adds to this chilling effect.
5. **The proposed rules would limit a company’s ability to employ non-U.S. resources in security-related activities.** Restrictions on information sharing within a company would limit the ability of companies to attract and retain well-qualified non-U.S. employees, whether in the U.S. or elsewhere, in security-related roles by requiring companies to assess citizenship and nationality and obtain export licenses in order for these employees to access controlled technology and source code. This problem would be most salient in the use of cross-border red/blue teams, but it would also arise even if entirely U.S.-based teams were used, due to the operation of BIS’ long-standing “deemed export” rule. In order to avoid these costs and added



layers of complexity, companies might have to forgo hiring the best and brightest security experts, ultimately harming their cybersecurity.

6. **Similar rules have not worked in the past.** In the technology space, the existing rules around export of encryption technology have done little to limit the proliferation of the technology, which has resulted in a series of revisions to BIS encryption rules as the government attempted to keep pace with rapid developments in the marketplace. The proposed rules appear to be taking the same approach to a similar problem, rather than rethinking this unsuccessful approach and developing a new model to address the proliferation of intrusion and surveillance items.

6. How the BIS Rules would Impact Companies' Ability to Improve Security

Our analysis of the proposed rules has identified a number of ways in which they could, as currently drafted, negatively impact our member companies' ability to improve their own security. Provided below are some real world scenarios that illustrate this negative impact.

Impact on Security Assessments

The proposed rules would have the most direct impact on red team/blue team exercises. These assessments simulate real-world attacks by using the same TTPs that attackers use, actively compromising systems, and exfiltrating data to test defenses. The red and blue teams could be located in multiple countries. The proposed rules would cripple our ability to perform red team exercises using non-U.S. resources because we might not be able to perform exfiltration of company-owned data from company-owned systems without first obtaining an export license. This would hinder our ability to rapidly test systems in response to the discovery of a new vulnerability. Likewise, the effectiveness of blue team exercises may be limited by our inability to share certain information and tools internally with non-U.S. resources without first obtaining an export license.

Impact on Security Tools

The most obvious impact on security tools from the proposed rules will be increased cost. Commercial companies that develop tools affected by these proposed rules will need to increase the cost of their tools to offset the additional cost of the regulatory burdens they impose. Since there is no intra-company exception in the proposed rules, if any of these companies have engineering resources based in locations to which they cannot export their own software without first obtaining an export license, they may have to relocate engineering positions to new and potentially more expensive locations. Many of these costs will be passed on to their customers in the form of increased prices for purchasing licenses. In addition, consulting firms that use similar tools will pass on this cost to their clients in the form of increased consulting fees for security consulting engagements.

There is also the potential for decreased variety and capability of available security tools. Increased cost and reduced speed to market for these tools may force commercial vendors to rethink their product portfolios to reduce their regulatory burdens. In addition, obtaining export licenses for items controlled by the proposed rules will increase the time required to release new capabilities in these tools. These delays could prove harmful, given the race to fix vulnerabilities once they are known to the public. Restrictions on the export of these tools to certain destinations could also hinder efforts to



mitigate security risks, potentially undermining the policy goals of the proposed rules by creating a new class of “soft” targets.

Impact on Information Sharing

The proposed rules will negatively impact both inter- and intra-company information sharing. The proposed rules make inter-company information sharing far more complex and much less effective. To avoid exporting controlled items, companies will need to determine the location and nationality of any company or individual with which they want to share information as well as determine which information is controlled and cannot be shared. Additionally, while it may be possible to determine in advance the companies or individuals with which a company wishes to share information, by their very nature the information or tools to be shared cannot be determined in advance, because the threat cannot be determined in advance. Thus, proactive steps to establish information sharing channels before a crisis occurs are precluded by the proposed rules. Given the need for growth of inter-company information sharing, any regulations that discourage information sharing are cause for significant concern.

For intra-company information sharing, the proposed rules make it nearly impossible for our U.S.-based incident response teams to share fully detailed threat information with company security operations center (SOC) personnel outside of the U.S. Sending security or testing tools related to these new threats may constitute an export requiring a license, even if it is only intended for defensive purposes. For example, if a U.S.-based incident response team discovers details on a new exploit and exfiltration software being used against its systems, it may not be able to send needed tools to incident response teams in Israel without first obtaining an export license. If the U.S.-based team applies for a license, critical systems may remain vulnerable while waiting for BIS to process the application.

Impact on Bug Bounties

One of the pieces of technical information that often comes from bug bounty reports is proof of concept software or tools that can be leveraged to validate the vulnerability. This essential technical information may constitute tools that are covered under the new rules. For example, when a researcher provides us (or we provide a software vendor) with a proof-of-concept exploit and additional technical data that outlines the underlying issue, steps of exploitation, and how the vulnerability might be used in a real attack, we are creating tools covered by these rules, even though our explicit intent is to help improve defenses. Without this complete, accurate, and full picture of a vulnerability, we cannot begin to secure our systems and software. Many of the vulnerabilities we receive are highly complex and difficult to reproduce. Thus, a usable bug bounty report might not just require information about the vulnerability, it might require the provision of software “specially designed” for the generation, operation or delivery of, or communication with “intrusion software” in order to demonstrate how a vulnerability could be exploited by an attacker. If we do not receive such tools, we may be unable to reproduce the vulnerability or validate that a designed patch actually addresses it.

In addition to limiting the data provided in bug bounty reports, we fear that the proposed rules would have an overall chilling effect on researchers' willingness to participate in these programs, whether due to actual licensing requirements, or due to widespread misconceptions over what kinds of tools and information are controlled under the proposed rules. As recent coverage in the trade press indicates,



many security researchers believe that sharing information on exploits is prohibited under the proposed rules, even though BIS has repeatedly stated that this is not correct. This chilling effect would lead to a direct reduction in the effectiveness of bug bounty programs. (See, e.g., “Student Claims Wassenaar Arrangement Prevents Him from Publishing Dissertation,” *Ars Technica*, July 2, 2015, available at: <http://arstechnica.com/security/2015/07/student-claims-wassenaar-agreement-prevents-him-from-publishing-dissertation/>; “Arms Control Treaty Could Land Security Researchers Like Me in Jail,” *Ars Technica*, May 27, 2015, available at: <http://arstechnica.com/security/2015/05/arms-control-treaty-could-land-security-researchers-like-me-in-jail/>)

How the Proposed Rules can be Improved

Since introducing the proposed rules, BIS has taken steps to clarify its position, but its interpretations of the proposed rules still remain unclear. For example, some of the FAQs appear to contain contradictions. As explained by the Electronic Frontier Foundation, “FAQ 10 clarifies that a researcher who has written a proof of concept for a vulnerability, 'code that takes advantage of the vulnerability,' would not be required to obtain a license before submitting the proof of concept to the vendor. But back up in FAQ 4, BIS told us that 'information on how to prepare the exploit for delivery' is controlled.” In addition, responses during conference calls show that BIS is still working to understand this space. We applaud BIS for noting that they are still gathering information about the industry; however, we believe that regulating such a complex industry without a deep understanding of how all of its pieces fit together is a dangerous approach.

Industry's reaction to the proposed rules demonstrates that, while BIS has good intentions, the proposed rules will have a number of unintended consequences. If BIS feels that it must regulate these tools, it should write the rules as narrowly as possible and with the goal of minimizing their adverse impact on the following key items:

- Inter and intra-company information sharing;
- Legitimate research that helps identify and fix vulnerabilities in the systems, software, and networks we use every day;
- Bug bounty and other similar programs that help businesses secure their systems, software, and networks with the help of vulnerability researchers;
- The need of companies and individuals to use security software to identify vulnerabilities in their own systems, software, and networks;
- The power that comes from researchers producing detailed reports on vulnerabilities to help developers fix their software; and
- Additional costs that will be incurred by companies and individuals who want to use security software to secure their systems, software, and networks.

To help address the concerns raised in this public comment, the members of the Internet Association recommend the following steps to bring the proposed rules in line with the harm we believe they are truly meant to target (*i.e.*, illegal surveillance and exfiltration of data from a target without authorization):

1. Introducing an intra-company exception;



2. Focusing on exfiltration and the use of cybersecurity items for unauthorized activities, not the items' technical capabilities;
3. Maximizing clarity around acceptable uses that do not require a license;
4. Including more detailed language in the regulations' text and preamble, similar to what has been included in the FAQs;
5. Sharpening the definition of “Intrusion Detection Systems” to include technologies that are both system and network-based, in order to avoid conflating network intrusion detection systems (NIDS)/man-in-the-middle (MITM) tools with surveillance tools; and
6. Providing better and more comprehensive guidance to help individuals and organizations understand their obligations under the proposed rules.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Michael Beckerman', written over a horizontal line.

Michael Beckerman
President & CEO
Internet Association

PUBLIC SUBMISSION

As of: 7/29/15 3:13 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-dy87
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0225

IBM Cyber Rule Comments 7-29

Submitter Information

General Comment

See attached

Attachments

IBM Cyber Rule Comments 7-29



U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
14th Street & Pennsylvania Avenue, NW
Room 2099B
Washington, DC 20230

IBM
600 14th St. N.W.
Washington, D.C. 20005

July 20, 2015

**Attention: Catherine Wheeler, Director
Information Technology Control Division**

Reference: RIN 0694-AG49

Re: Comments on Rulemaking Concerning Revision and Clarification of U.S. Proposal for Implementation of Wassenaar Agreement Export Controls on Intrusion and Surveillance Items

Dear Ms. Wheeler,

On behalf of International Business Machines Corporation (“IBM”), we are submitting these comments in response to the Bureau of Industry and Security (“BIS”) May 20, 2015, request regarding the proposed implementation of the December 2013 Wassenaar Arrangement (“WA”) Plenary Agreement on Export Control of Intrusion and Surveillance Items (80 Fed. Reg. 28853 (May 20, 2015)) (“Proposed Rule”). These comments are timely submitted by the due date noted in the Proposed Rule.

IBM provides information technology products and services to customers in over 175 countries, and employs more than 379,000 persons across 75 countries worldwide. 2014 revenues were \$92 billion, of which over 60 percent was generated outside the United States. Consistent with today’s era of unprecedented technological change, IBM is reinventing its business and dynamically shifting focus toward an analytics, mobile, social, and cloud driven portfolio. As part of this strategy, IBM has created a business unit solely focused on cyber security.

IBM operates one of the world’s broadest cyber security research, development, and delivery organizations. Among its offerings, IBM’s security platform provides security intelligence to help organizations – including both businesses and government agencies – holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more.

This breadth of experience affords IBM unique insight into today’s most pressing security challenges – as well as the opportunity for U.S. leadership to address these challenges. As the reliance on advanced information technology continues to grow with the transition to cloud computing and data analytics, it is imperative that security for these systems be on the cutting

edge. Impediments to the development of robust security measures will hinder U.S. national and economic security. The comments on the Proposed Rule offered by IBM are intended to assist BIS in avoiding such impediments, while addressing the U.S. national security interests appropriately identified by BIS in the Proposed Rule.

Summary

Although well-intended, the Proposed Rule creates a complicated regulatory structure that injects a great deal of uncertainty around the sale, development and use of certain classes of cyber security products. Given its ambiguity, the resulting complex interpretations of the Wassenaar definitions will result in many companies seeking reviews and opinions about their products, their development scenarios and use of technology and commercially available third party products. Further, the Proposed Rule creates a new and significant licensing requirement. This licensing requirement will greatly inhibit the free exchange of information that enhances cyber security. Unlike regulatory policy in other areas of the Export Administration Regulations (“EAR”), which utilize a license exception framework, this proposed rule would overlay a new and very challenging framework of untested regulation for both industry and BIS licensing staff. As a result, IBM anticipates that there will be delays with the deployment of cyber products, delays with the exchange of information about threats, and a chilling effect on cooperation between parties due to concerns about penalties and compliance. Such a scenario will benefit neither U.S. national security interests nor U.S. industry, as cyber threats continue to multiply. Rather, this scenario will run counter to openness and speed, attributes needed to combat threats in cyber space. IBM therefore urges that this Proposed Rule be withdrawn and consideration be given as to revisiting this issue within the Wassenaar Arrangement in order to significantly narrow the language that was adopted in 2013 and more precisely target items that may require control. If BIS nonetheless proceeds with the Proposed Rule, in IBM’s view, it is imperative that BIS focus any new controls on the cyber security items with the greatest potential for abuse, utilizing a control framework that leverages the EAR’s existing license exception approach.

Effects on Internal Use

As companies, including IBM, increasingly transform themselves into a cloud enterprise, more and more infrastructure, platforms, and applications are being virtualized and placed in the cloud. Everything from employee communications to corporate intellectual property assets to customer data is in the cloud, which operates on a secure worldwide integrated network. For this reason, companies, including IBM, need to maintain a highly robust and comprehensive strategy for security worldwide.

Many companies, including IBM, use both third party and internally developed security products, utilities and tools. The worldwide deployment process for these items is dynamic and, given the sophistication of threats, must be agile to respond to the latest exploits, malware or viruses. In addition to the use of products, utilities and tools, many companies, including IBM, conduct “ethical hacking” internally to test the security of portions of the network, drawing on the best internal experts from around the world. This creative and forward-looking process is an absolute necessity in the cyber world. The proposed licensing requirements would create a significant regulatory burden on simply maintaining the security of a company’s network -- for

ourselves and our customers. Requiring an export license to develop a tool, share information, collaborate on a solution in real time or even install a third party vendor product simply is not compatible with adequately protecting the current online environment where threats move at cyber speed.

As a result, IBM believes the Proposed Rule must be fundamentally reconsidered. IBM would strongly suggest that any proposed rule distinguish between permissible defensive uses of certain classes of products (e.g., penetration testing tools), both for internal use and for our customers. IBM believes that a proposed regulation should not be constructed to penalize legitimate defensive uses that our customers are requesting as part of our service to them. In addition, if BIS decides to pursue these controls, IBM suggests that, at a minimum, a Global Intracompany License Exception be created to permit global companies, like IBM, to maintain the current freedom and flexibility to research, develop, test, and deploy solutions to ensure the health and security of their internal networks.

Effects on Research and Information Sharing

In IBM's experience, a single company cannot expect to be successful, on its own, in combating cyber-attacks, given the scale of the cyber-criminal community and variety of threats. Research and information sharing (both public and non-public) are vital to ensuring network security, protecting sensitive data, and securing intellectual property. Limitations on the free flow of information weaken security for IBM, the IT industry as a whole, and the customers of this industry, including the U.S. government, by slowing the dispersal of knowledge about threats. The Proposed Rule will create such limitations and greatly inhibit the free exchange of information by creating the need for export licenses and deemed export licenses. As with most companies, IBM research teams gather information from a wide variety of sources, including global teams, and restricting or even slowing the exchange of information among these sources would inevitably weaken the overall cyber threat response infrastructure.

Moreover, IBM has moved to share this information externally. The value of IBM's cyber security research effort can be demonstrated by a threat intelligence sharing platform that IBM established in 2015 – IBM's X-Force Exchange. This platform allows for registered users to research security threats, aggregate intelligence, and collaborate with peers. This collaborative platform provides access to volumes of actionable IBM and third-party threat data from across the globe, including real-time indicators of live attacks, which can be used to defend against cybercrimes.

In general, collaborative efforts – on platforms like X-Force Exchange or in customer/vendor partnerships – by their very nature will result in outcomes that produce some technology or technical information that will be exchanged between parties. IBM foresees such collaboration on addressing cyber threats being negatively affected by the licensing provisions of the Proposed Rule, which likely will have a chilling effect on information sharing. Moreover, for real-time threats, it would likely be impossible to define in advance in a license application what IBM or a customer or vendor might transfer in terms of a solution to a cyber-attack, as both the nature of these attacks and effective responses are constantly evolving. These efforts may start out as pure research that does not require a license, but they can morph into more advanced work that could

potentially cross over into licensable activity. Moreover, parties often are not immediately interested in publishing what they discover for a variety of commercial, privacy, or other reasons.

Indeed, IBM believes that the Proposed Rule runs directly counter to the policy of encouraging the sharing of cyber threat information and security best practices put forward in Executive Order 13691 of February 12, 2015, as well as in several pieces of proposed legislation currently under consideration in the U.S. Congress. Further, in Executive Order 13691 and the related White House Fact Sheet of July 9, 2015, on the Administration's 2015 Cybersecurity Efforts, the Administration has emphasized that information exchange and private sector cooperation is paramount to addressing cyber security vulnerabilities. Moreover, in addition to encouraging this cooperation, the various legislation does define permissible defensive activity or uses, which is important to securing networks. IBM encourages BIS to give careful consideration to whether the Proposed Rule is consistent with these efforts.

IBM suggests that the Proposed Rule be recalibrated so as not to discourage such information sharing and collaboration by the legitimate business community. IBM believes that a Global Intracompany License Exception would also apply to internal use for cyber security research and product development. In IBM's view, the U.S. government would benefit more from an approach that enables the U.S. information technology ("IT") industry to constantly innovate in the security space, especially in light of the fact that many U.S. government agencies leverage the services of U.S. IT companies.

Effects on IBM Products and Services

The new proposed rule would create a massive new structure to individually license each product sale, development activity and use case for certain products that meet the newly defined elements of the proposed Export Control Classification Numbers ("ECCNs") 4A005, 4D001, 4D004, 4E001 and 5A001.j.

IBM strongly suggests that any new controls on cyber security products follow an approach similar to that employed by BIS for encryption items. The current regulatory structure for encryption items, with its license exception format whereby products are classified once and controls attach for certain end-use customers or countries, is a successful and rational mechanism. Products of a certain type require an export license to most government end users and are banned to end users in certain countries (i.e., the Country Group E:1 countries). Further, sales of certain products must be reported to BIS and are potentially subject to checks or audits. Similarly, any new controls on cyber security products should cover a narrowly drawn, clearly defined list of types of products and should be constructed in the same manner as the existing license exception framework for encryption items. IBM further suggests that the controls be limited to platforms for launching attacks. Such a structure will achieve BIS' goal of limiting access to the products posing the greatest cyber threat and allow for the creation of predictable and manageable classification rules for BIS and private industry.

IBM currently believes that our products do not meet the identified attributes in the definitions used in in ECCNs 4A005 and 4D004; however, we are very concerned that these definitions are open to a broad range of interpretations. IBM believes that performing vulnerability scanning

and “ethical hacking” services for a customer could be potentially affected depending upon the type of activity. Development and deployment of these services are on a worldwide basis and the tools deployed would be potentially captured by the Proposed Rule. While the number of services potentially captured may be small relative to IBM’s overall business, customers find these services to be critical to their security posture. In addition, the possibility of new products and services being subject to the Proposed Rule in the future is clearly a concern, as IBM cannot always predict market demands for a service or product.

Conclusion

IBM believes that a fundamental rewrite of the Proposed Rule is necessary in order to promote the regulatory objective to restrict certain products and technologies without having an outsized impact to the IT industry and its efforts to constantly improve the security of products and services in a timely manner. The sale of products, their development, their internal use, and information sharing around the latest threats could all be drastically impacted by the licensing requirements. From a practical perspective, this is likely to be unworkable. Threats will be discovered in real time, with immediate action and collaboration needed to counteract those threats in real time. Introducing an export license requirement into this process will only serve to hinder the goal of achieving greater cybersecurity, rather than advancing it.

With the global nature of the IT industry and cyber-crime, it ultimately would be counterproductive to place controls around security research, product development and security services. Doing so would negatively impact the creativity and innovation that is required in this area.

We thank you for the opportunity to comment.

A handwritten signature in black ink, appearing to read "Edward A. Bond". The signature is fluid and cursive, with a large initial "E" and "B".

Edward A. Bond
Director, Export Regulation Office
Government & Regulatory Affairs
IBM Corporation

PUBLIC SUBMISSION

As of: 7/29/15 3:26 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-zgvj
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0226

Howard Grodin

Submitter Information

General Comment

See attached

Attachments

Howard Grodin

Sharron Cook

From: Howard Grodin <hgrodin@gmail.com>
Sent: Monday, July 20, 2015 12:06 PM
To: PublicComments
Subject: RIN 0694-AG49

Dear Sir or Madam,

I offer the below comments, solicited as part of your review process, out of genuine concern for both the vendors of Penetration Testing tools as well as the legitimate end-users, both corporate and individual.

I strongly believe that the proposal as written is much too broadly worded and puts the legitimate use of, purchase and sale of Penetration Testing tools at risk of harming its legitimate uses in protecting business and consumers from vulnerability exploitations.

Sincerely,

Howard Grodin

Information Security Professional

RE: RIN 0694-AG49 <<https://www.federalregister.gov/r/0694-AG49>>

PUBLIC SUBMISSION

As of: 7/29/15 3:27 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-64pw
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0227

HackerOne Katie Moussouris

Submitter Information

General Comment

See attached

Attachments

HackerOne Katie Moussouris

Sharron Cook

From: Katie Moussouris <katie@hackerone.com>
Sent: Tuesday, July 21, 2015 12:39 AM
To: Sharron Cook; PublicComments
Subject: Re: Comments on BIS-2015-0011

Forwarding the comments to the publiccomments email address as well.

Katie

On Jul 20, 2015 21:14, "Katie Moussouris" <katie@hackerone.com> wrote:

Thank you for providing an opportunity for public comment on this proposed rule.

About HackerOne:

Created by security leaders from Facebook, Microsoft and Google, HackerOne is the first vulnerability coordination and bug bounty platform. We empower organizations to protect consumer data, trust and loyalty by working with the global security research community to uncover the most relevant security issues. HackerOne is a venture-backed company with headquarters in San Francisco.

On July 2nd, 2015, HackerOne reached 10,000 valid security vulnerabilities resolved on our platform - that's 10,000 fewer ways for attackers to exploit users, steal data, and cause damage. The first bug was filed on the HackerOne platform 20 months ago, and today over 250 organizations resolve hundreds of bugs each week thanks to the help of thousands of researchers around the world. Nearly \$4M USD in bounties have been paid through our platform as of July 2015.

Summary of Comment:

We believe the proposed rule would negatively impact the ability for organizations to defend themselves, and curtail the growing defensive vulnerability coordination market where our business is playing a defining role, while not meeting the intended goal of protecting human rights. Our recommendation is to work with BIS to help revise the language of the proposed rule, to limit the scope and make these well-intentioned goals work without unintended consequences. Ultimately, we believe that the countries involved with the Wassenaar arrangement will have to revisit the inclusion of "intrusion software" to focus more on the action taken by the malware, such as exfiltration or stealing of data.

We believe that the wording of the proposed rule as it stands will break the fundamental primitives of vulnerability coordination and disclosure, and create an undue burden for defenders and security researchers alike. The US will be at a trade and intellectual advancement disadvantage under these circumstances.

Specific concerns around vulnerability coordination and disclosure:

An important overlooked and misunderstood part of the Wassenaar debate is that vulnerability disclosure itself—with or without cash bug bounty payments—is threatened by the new rules, despite the stated intent of the authors of the regulations to leave vulnerability research and disclosure untouched.

As BIS states in their FAQ <<http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faq>> :

“4. Will the rule control vulnerability research as well as research on exploits?

...the proposed rule would control the following, among other things:

1. Information "required for" developing, testing, refining, and evaluating "intrusion software", in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information. [editor's emphasis]
2. Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.
3. The development or production of the command and delivery platform itself.”

The FAQ further states that public disclosure provides an exemption:

“..export controls do not apply to any technology or software that is "published" or otherwise made publicly available.

Thus, only that part of the technology that is peculiarly responsible for meeting the definition of "intrusion software," and which is not publicly available, would be controlled.”

But not all parts of vulnerability information sent to a vendor are necessarily publicly disclosed.

Vital pieces of technology, for example a brand new exploitation technique that may have been used in the Proof of Concept code delivered to a vendor as part of a vulnerability disclosure process, would be subject to export control if the technique were to remain private. An exploitation technique is distinct from a vulnerability or an exploit. Think of it as the blueprints to build the weapon, rather than the weapon itself.

An example of an exploitation technique <<http://www.contextis.com/resources/blog/windows-mitigation-bypass/>> was discovered and reported to Microsoft to win the very first \$100,000 mitigation bypass bounty <<http://blogs.technet.com/b/bluehat/archive/2013/10/08/congratulations-to-james-forshaw-recipient-of-our-first-100->

000-bounty-for-new-mitigation-bypass-techniques.aspx> , which helped improve the defense of future versions of Microsoft software. Two years ago, I wrote in a blog that “learning about new mitigation bypass techniques helps us develop defenses against entire classes of attack. This knowledge helps us make individual vulnerabilities less useful when attackers try to use them.”

This confusion and concern around what does and doesn’t fall under export control won’t just affect security researchers. Vendors receiving vulnerability reports will have to apply for “deemed export licenses <<https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports>> ” themselves in the case where they employ foreign nationals that may come in contact with export-controlled technology.

This burdensome license application process would have to happen even if the researcher was in the U.S. disclosing to an American vendor who employs foreign nationals. Also taken from the BIS FAQ: “There is no license exception for intra-company transfers or internal use by a company headquartered in the United States under the proposed rule.”

Granting an exception for “intra-company transfers” wouldn’t solve the problem for cases when one vendor needs to work with other companies in order to address the security issue. Essentially, the proposed rule would break the fundamental ability for vendors to defend themselves, which leaves everyone more vulnerable to the kinds of attacks the regulation was designed to prevent.

Exploits Can Be Used for Good or Evil

There’s a conundrum when it comes to exploits and other potentially malicious software. For human rights advocates, software like DaVinci from Hacking Team that bypasses security protections, hides from anti-virus and other malware detection tools, and spies on the victim, represent a threat to human life when used by repressive regimes. But for security researchers, the same offense techniques that are developed to bypass existing computer security measures are used in research to highlight weaknesses in order to fix the vulnerable software.

These identical techniques simply can’t be logically separated from the exploit techniques that are used by criminals and nation states in spyware tools. In other words, these technologies are dual-use—aiding defenders who are testing their security and used by attackers who are up to no good.

Getting in the way of defense is not the goal of regulations, yet they stand to deal blows to that process in ways that will lead to more victims in the end, due to the overall weakening of Internet defense.

Those who wish to create tools and use or distribute them to cause harm will continue to do so with the impunity that was revealed in the internal communications of the hacked Hacking Team. No regulation will stop them. It is our job to collectively ensure that no regulation stops defenders.

Katie Moussouris

Chief Policy Officer

HackerOne

PUBLIC SUBMISSION

As of: 7/29/15 3:29 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-rtos
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0228

Google Comment Neil Martin 7-29

Submitter Information

General Comment

See attached

Attachments

Google Comment Neil Martin 7-29

Re: RIN 0694–AG49 - Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Sir/Madam:

Google welcomes the opportunity to comment on the proposed rule for cybersecurity export controls, particularly relating to intrusion software and surveillance items. On May 20, 2015, the Commerce Department's Bureau of Industry and Security ("BIS") published a proposed rule in the Federal Register entitled Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49). (See 80 Fed. Reg. 28853.) This comment will respond to specific questions posed by BIS in the proposed rule. It will also raise areas of concern and offer recommendations.

Section One: The Proposed Export Controls Relating To Intrusion Software Are Broad In Scope

The term "intrusion software" is incredibly broad. As a result, the proposal for related controls in 4A, 4D, and 4E of the Commerce Control List ("CCL") may capture more goods, software, and information than BIS has anticipated.

In the proposed rule, "intrusion software" is defined as: "[s]oftware" "specially designed" or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device, and performing any of the following:

- (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
- (b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

Notes:

1. "Intrusion software" does not include any of the following:
 - a. Hypervisors, debuggers or Software Reverse Engineering (SRE) tools;
 - b. Digital Rights Management (DRM) "software"; or
 - c. "Software" designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.
2. Network-capable devices include mobile devices and smart meters.

Technical Notes:

1. 'Monitoring tools': "software" or hardware devices, that monitor system behaviors or processes running on a device. This includes antivirus (AV) products, end point security

products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls.

2. 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

The crux of the issue is that the exploitation of any software "bug" (as that term is commonly understood within the industry) will almost certainly alter the standard execution path of a program and therefore trigger the criterion in paragraph (b) of "intrusion software." A piece of software is a series of instructions that are followed in sequence. The very nature of a bug allows someone to change the program's behavior to do something that a developer did not intend. Also, computer software regularly allows users to modify the execution path through user input or user-supplied configuration files. Exploitation of a bug will almost surely alter the standard execution path of a program, and the modification of the execution path by externally-provided instructions is common, thus bringing almost all software bugs into the scope of the term "intrusion software," which impacts the scope of ECCNs 4A005, 4D004, and 4E001.

Additionally, paragraph (a) of "intrusion software" applies to tools vital in identifying computers on a network that have been compromised. Google has software and hardware designed to provide security functionality that could become controlled under BIS' proposed rule. For example, certain internal security software used to detect and eject intruders on the network was intentionally designed to avoid detection by malicious software that could be running on a system. This also has the effect of hiding from antivirus programs. Such security software performs all of the functions listed in paragraph (a) of "intrusion software." Internal software programs used to manage the incident response software would fit within the parameters of 4D004. Operating incident response software and the software platforms managing those tools are critical for identifying computers on a network that have been compromised.

In particular, proposed ECCN 4E001.c is very broad in scope. That ECCN would control "[t]echnology" "required" for the "development" of "intrusion software." Unless software engineers write perfect code on their first attempts, the code may contain flaws. Some of these flaws may include being vulnerable to "intrusion software" as defined by BIS' proposed rule because they allow an alteration of the program's standard execution path. When other engineers and security personnel perform code reviews, they may provide comments to the original code writer about any vulnerabilities they find. Based on their specific content, some of these comments could be properly classified as 4E001.c. It is common for companies to create references or details about how to exploit a vulnerability in their own software and to communicate that information. The information could appear in codebases, bug tracking systems, email conversations, communication systems, live conversations, etc. The information could also relate to zero-day exploits. BIS has not defined this term, and it is susceptible to multiple potential definitions, but we assume that BIS is referring to non-public vulnerabilities.

BIS' FAQ on the proposed cybersecurity rule does not help to limit the scope of 4E001.c. FAQ number 4 states that the "proposed rule would not control the following: 1. Information on how to search for, discover or identify a vulnerability in a system, including vulnerability scanning; 2. Information about the vulnerability, including causes of the vulnerability" and that "the only technology controlled is the technology that is 'required for' and peculiarly responsible for achieving or exceeding the control level." (See <http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>.) We respectfully disagree to some extent with the conclusion of this FAQ. Although it is true that not all such information is necessarily "required" and peculiarly responsible for meeting the criteria in 4E001.c, certainly some information, especially about the causes of the vulnerability, could be peculiarly responsible and "required" for the development of a software vulnerability. The analysis would depend on the specific circumstances involved. The amount of information falling within the parameters of 4E001.c will be especially large if BIS adopts its proposed definition of "peculiarly responsible" in its proposed rule for "Revisions to Definitions in the Export Administration Regulations," which is part of the Administration's Export Control Reform Initiative. (See <http://www.gpo.gov/fdsys/pkg/FR-2015-06-03/pdf/2015-12843.pdf>.) Under the "catch" and "release" approach of the proposed definition of "peculiarly responsible," very little information about a software vulnerability would likely qualify for the narrow "release" provisions. Ultimately, a tremendous amount of information about software vulnerabilities will fall within the current parameters of "required" and "peculiarly responsible," and even more information would be pulled into the scope of those terms if BIS adopts its proposed definition of "peculiarly responsible."

Section Two: BIS' Questions Posed in the Proposed Rule

This section answers the various questions posed by BIS in the Federal Register.

Question 1: How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications: a. How many additional applications would be for products that are currently eligible for license exceptions? b. How many additional applications would be for products that currently are classified EAR99?

If BIS adopts this proposed rule, Google will have to submit license applications to export 4D004 software, related 4E001 "technology," 5A001.j hardware, 5D001 software, and related 5E001 "technology" to every country outside of the U.S. and Canada in which it has offices. Currently, Google can export such material from the U.S. to these offices without restriction either under license exception ENC or because the material is classified as EAR99.

Google has security tools used internally that would be controlled under 4D004. For instance, certain internal software tools used to scan mobile apps for malware prior to being made

available on Google Play would fall within the scope of 4D004. Such software may not already be located in all Google offices, or updated versions of such software may need to be exported to those offices, which would require a license under the proposed rule to all offices other than those in the U.S. or Canada. The security of our users depends on Google being able to act quickly when vulnerabilities are discovered. Historically, BIS has taken several months to process a given export license application submitted by Google. We are concerned that BIS is not staffed adequately to handle the enormous volume of new applications Google would need to submit if BIS adopts this proposed rule. It would create an unreasonable risk to users of our products and services if Google needed to wait months for BIS to issue an export license to a given country after a relevant security issue has been discovered or a specific need to transfer 4D004 software to a new country has been identified. Any regulatory delay in addressing security vulnerabilities is unwarranted.

Google potentially has 4E001.c “technology” spread widely across the company. 4E001.c controls “[t]echnology” ‘required’ for the ‘development’ of ‘intrusion software.’” As mentioned previously, software code may contain flaws, some of which may include being vulnerable to “intrusion software” as defined by BIS’ proposed rule. When other engineers and security personnel perform code reviews, they may provide comments to the original code writer about any vulnerabilities they find. Based on their content, some of these comments could be properly classified as 4E001.c. These comments could appear in code bases, bug tracking systems, email conversations, communication systems, live conversations, etc. It is impossible to locate all specific instances where such technology presently exists within the company or where it may be created in the future, especially given the broad definition of the term “intrusion software.” It will be impossible to predict specifically when 4E001.c “technology” will come into existence or be exposed to a specific engineer. In order to protect the security of Google users worldwide, when the need to transfer such technology to other Google offices arises, the security of our users depends on the company being able to act quickly. It would create an unreasonable risk to users of our products and services if Google needed to wait several months for BIS to issue an export license to a given country after a relevant security issue has been discovered or a specific need to transfer 4E001.c technology to a new country has been identified. Accordingly, broad export authorizations will be required in order to preserve Google’s ability to identify and fix security issues in its products as quickly as possible.

In addition to export licenses for its own offices, Google would require licenses in order to engage with a variety of third parties in the area of intrusion software. It is unclear at this time how many export licenses would be necessary, but examples of such transactions include engaging vendors in the security and threat intelligence space; communicating with security counterparts at other companies, like Amazon, Apple, Microsoft, Mozilla, Yahoo, and others; and working with security researchers who report vulnerabilities to Google. Even purely domestic transactions could have deemed export license requirements for both Google and the parties with whom we interact. The proposed rule relating to intrusion software and its imposition of a license requirement for exports to destinations other than Canada will result in slowing the speed at which exporters can fix security holes in their products and help other

companies fix holes in theirs. This regulatory environment would be detrimental to the users of technology products and the companies that make them. However, it would also have the unintended consequence of enabling bad actors seeking to exploit vulnerabilities since technology companies will not be able to address security issues as quickly as they can today.

Indeed, the license requirements in the proposed rule run counter to the President's executive order that "In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

BIS has indicated a licensing "policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities." These terms are susceptible to multiple potential definitions. However, we believe it likely that BIS is referring to vulnerabilities that have not been disclosed publicly. A great deal of work conducted internally or with external security researchers involves non-public vulnerabilities. Related technical data would frequently be classified under 4E001.c. It would seem that such a licensing policy would conflict with the President's executive order cited above and with Google's need to fix vulnerabilities in its products. If BIS were to prohibit Google from internally distributing information about non-public vulnerabilities to offices outside of the U.S. and Canada or to anyone who is not a U.S. or Canadian national, it would have grave security consequences for the company and for users of our products. Accordingly, we request that BIS revisit this policy.

Additionally, Google has internally-created security tools in the U.S. that would be controlled under 5A001.j or 5D001 and related "technology" that would be controlled under 5E001. Google may use hardware-based or software-based intrusion detection systems (IDS) that capture network packets, process data at the application layer, index it, and cross-reference against known indicators of compromise (as hard selectors). These tools are used to detect suspected malicious network activity. Some of the software tools may be open sourced, but others will be left as proprietary, closed source code. These hardware and software tools could be exported from the U.S. to any Google datacenter or office. As a result, Google would need to submit to BIS dozens of export license applications for such transfers.

Question 2: How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

Under the proposed rule, Google would need to submit thousands -- maybe even tens of thousands -- of license applications in order to authorize deemed exports and deemed reexports. Historically, BIS has taken several months to process a given deemed export license application submitted by Google. Again, we are concerned that BIS is not staffed adequately to handle the high volume of new deemed export license applications that Google would need to

submit if it adopts this proposed rule. Tens of thousands of foreign persons work at Google. As described earlier, it's possible that any engineer could theoretically write software code susceptible to intrusion software attacks unless the code is fixed. Any engineer reviewing another person's code could identify a security problem in that code, provide feedback to the code writer, provide information proving that the security problem is real, provide code proving that the security problem is real, provide information about how to fix the problem, etc. Some of this information would constitute 4E001.c technology. It is impossible to predict which specific Google employees would either write or review code in a manner resulting in the creation of 4E001.c technology or when it will occur. Additionally, copies of such code and related development technology already exist due to code reviews that occurred in the past, comments in code written in the past, emails that were written, etc. Therefore, Google would need to obtain licenses authorizing exports to all foreign persons (besides Canadian nationals) working at the company as an engineer. It would be unrealistic to attempt requiring all non-Canadian foreign persons to simply stop writing software code that could theoretically become vulnerable to intrusion software (i.e., mandate writing perfect code on the first attempt), never review previously-created software code and related technology, or not to discuss security vulnerabilities.

Some deemed export license applications would include transfers of 4E001.c technology to people outside of Google. As mentioned in the answer to Question 1, transactions with external parties include engaging vendors in the security and threat intelligence space; communicating with security counterparts at other companies, like Amazon, Apple, Microsoft, Mozilla, Yahoo, and others; and working with security researchers who report vulnerabilities to Google.

Broad export authorizations will be required in order to preserve Google's ability to identify and fix security issues in its products as quickly as possible. People at Google will need to discuss issues relating to "intrusion software," which may entail the transfer of 4E001.c technology. It would be impractical to delay submitting license applications for deemed exports to non-US and non-Canadian nationals until live issues arise. Doing so would create an unacceptable delay in fixing security issues while waiting several months for export licenses to be issued for specific workers. Any delay puts the security of Google users at risk unnecessarily.

Additionally, as stated earlier, Google has created its own internal security tools that would be controlled under 5A001.j or 5D001 and whose related "technology" would be controlled under 5E001. These tools are used to detect and mitigate suspected malicious network activity. Some of the software tools may be open sourced, but others will not. Access to controlled source code or technology would be needed by at least several hundred employees. Accordingly, Google would need to submit to BIS a high volume of export license and deemed export license applications.

However, the imposition of any license requirement for exports and deemed exports facilitating security defense runs counter to the President's executive order that "In order to address cyber threats to public health and safety, national security, and economic security of the United

States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.” (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

Question 3: Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company’s ability to protect your own or your client’s networks? If so, explain how.

Google has a global network and datacenter presence, which is designed to serve users in multiple countries. If Google were unable to deploy controlled 5A001.j hardware or equivalent software to locations outside of the U.S. and Canada, it would be unable to adequately monitor for threats on infrastructure outside of the U.S. and Canada. Such a deficiency could render Google unable to continue to provide the highest security standards for security and privacy, not only for foreign locations, but also the intra-connected networks inside the U.S. and Canada.

The proposed controls relating to “intrusion software” and accompanying export licensing policy would severely restrict critical security protections, real-time security vulnerability research, and security product development and adoption for U.S. companies, academia, nonprofits, and individual. The proposed export control, via the definition of “intrusion software,” would impose severe restrictions that would undermine U.S. security.

First, under the proposed rule, sharing a variety of security tools and information about vulnerabilities within a single company will be restricted. Even transactions happening entirely within the U.S. could require deemed export licenses if certain security-related source code or technical data is shared with someone who is not a national of the U.S. or Canada.

Second, the sharing of threat information between companies would be severely hampered, creating a requirement in some cases for obtaining export licenses before being able to warn other companies about ongoing threats. This would impact both informal sharing and formalized cybersecurity initiatives by the U.S. Computer Emergency Readiness Team (US-CERT), the U.S. Sector Coordinating Councils, Information Sharing and Analysis Organizations (ISACs), and new initiatives like Google’s Project Zero or Facebook’s ThreatExchange.

Third, the rule would significantly slow the development, operation, and functionality of automated security vulnerability identification and reporting tools, APIs, or backend systems that companies build into their own products to protect users, services, and physical infrastructure. Similarly, it would slow the deployment of security patches for products impacted by intrusion software (e.g., Heartbleed and POODLE) across both the private and public sectors. Even email accounts set up by companies, nonprofits, or the public sector to specifically receive security threat and vulnerability information from the general public could end up storing export-controlled information under the proposed rule.

Fourth, the environment for purchasing and selling security threat intelligence tools would be placed at risk, ranging from export control limitations on the vendors that companies use for security/threat intelligence to the products that companies can sell to provide threat intelligence functionality. In addition, the types of audits that companies would be allowed to perform on third-party vendors systems would be hampered if information relating to intrusion software is detected and delay how quickly that information can be conveyed back to the vendor for repair.

Lastly, the work of the security research community would be severely restricted, especially for security vulnerability researchers at U.S. and international universities, who currently share threat information directly with U.S. companies (e.g., zero-day vulnerabilities) over email. In addition, the events hosted by this community would face potential restrictions regarding the real-time sharing of information -- including bug bounties and hackathons -- which are created to specifically identify security exploits and then share that information back with the affected companies as quickly as possible.

In order to comply with the proposed rule, Google would be required to seek thousands of licenses authorizing the export and deemed export of materials relating to "intrusion software," which would consume a great deal of compliance resources that could be directed to more useful purposes. Many technology producers may not be staffed adequately to manage such an extraordinary increase in the number of export licenses that would be required under the proposed rule.

The process of preparing export license submissions, waiting for license approvals, maintaining licenses, submitting renewal license applications, etc. can only serve to delay, not accelerate, efforts by security professionals and engineers to fix vulnerabilities found in Google's and others' products. Such a result will place vast numbers of technology users at risk unnecessarily. Therefore, this proposed rule does not serve the President's desire that "In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

Further, the strict export controls and licensing policies in the proposed rule may create an incentive for security researchers to make their discovered vulnerabilities publicly available, which would serve to eliminate or significantly reduce the researchers' export compliance burdens, in lieu of responsibly disclosing them to technology producers first. In such an environment, technology producers would not be able to develop fixes for their products and have them in place prior to the public release of the vulnerability. Depending on the vulnerability, this could result in millions -- or billions -- of users being exposed to exploitation by bad actors for significant periods of time while technology companies scramble to roll out fixes. It would be

a perverse outcome if an export regulation intended to make people more secure were actually to result in billions of technology users across the globe becoming persistently less secure.

Question 4: How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

It is unclear how much time would be required to answer the questions in proposed paragraph (z) to Supplement No. 2 to Part 748 of the EAR. To the extent that Google needs to submit license applications for future, speculative vulnerabilities (e.g., in order to transfer 4E001.c “technology” to Google offices outside of the U.S. or Canada or to foreign persons who are not Canadian nationals), it simply would not be possible to provide such information.

Even when such information would be available, in cases where a new vulnerability were discovered, it would be an onerous process to gather, compile, and document this information for inclusion in an export license application or deemed export license application. More importantly, this process would distract from and delay security engineers’ efforts to actually address a live vulnerability. This proposed rule does not facilitate the President’s desire that “In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.” (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.) Google recommends that BIS eliminate this requirement -- and any other requirement that could delay fixing cybersecurity issues.

Section Three: Additional Comments

Google provides the following supplemental comments.

- 1. BIS should create a license exception authorizing intra-company exports and deemed exports of goods, software, and technology relating to cybersecurity items and transfers to “U.S. subsidiaries” akin to the provisions in license exception ENC.**

Historically, the process of preparing a license application, submitting it, and obtaining approval from BIS takes several months. With the incredible volume of additional license applications that would be required under the proposed rule, we would anticipate an increase in BIS’ license processing times. As discussed above, Google, other technology providers, and technology users around the world will be put at unnecessary risk if BIS

requires that exporters obtain licenses in order to perform work intended to make users more secure. Such work may be performed by employees and interns of Google; it also may involve contractors. It may also require working with other companies headquartered within the U.S. as well as their foreign subsidiaries and foreign national employees, interns, and contractors. Part 740.17(a) of the Export Administration Regulations (license exception ENC) provides broad authorization for the export of encryption items within and between U.S. companies and their subsidiaries. BIS should create an equivalent license exception authorizing the export and deemed export of controlled items related to intrusion software and surveillance items. Such an authorization will enable U.S. technology companies to address vulnerabilities and maintain network security without the administrative overhead required to prepare and maintain thousands of export licenses. Even more importantly, a license exception would authorize immediate exports and deemed exports without having to wait for approval from BIS. Such delays only serve the ends of bad actors interested in exploiting vulnerabilities and not technology companies making products for billions of users, the people who seek to protect those users' security (like the security research community), or the users themselves. This requested license exception would be consistent with the President's directive that "private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

- 2. BIS should create a license exception authorizing exports, reexports, deemed exports, and deemed reexports of controlled items relating to intrusion software when such transfers are made:**
 - a. to the manufacturer of the vulnerable product, its employees, or its contractors wherever located;**
 - b. to any other agent of the vulnerable product's manufacturer, wherever located;**
 - c. where the purpose of the export is to report vulnerabilities to manufacturers or their agents and have the vulnerabilities fixed.**

Although a license exception akin to ENC is necessary for exporting items related to intrusion software, it is not sufficient in and of itself. Many producers of popular technology products are headquartered outside of the United States. For instance, many participants in the Open Handset Alliance are located outside of the U.S. (see <http://www.openhandsetalliance.com/index.html>). If a vulnerability is discovered by a U.S. person in a product whose manufacturer is not in the U.S. or Canada, that person should be able to report the vulnerability to the manufacturer without restriction even if doing so results in the transfer of controlled material, like 4D004 software or 4E001.c technology. Again, a license exception would authorize immediate exports and deemed exports without having to wait for approval from BIS. Such delays only serve the ends of

bad actors interested in exploiting vulnerabilities and not technology companies making products for billions of users, the people who seek to protect those users' security (like the security research community), or the users themselves. This license exception would be consistent with the President's directive that "private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

- 3. BIS should create a license exception authorizing exports, reexports, deemed exports, and deemed reexports of controlled items relating to intrusion software when such transfers are made by product manufacturers, their employees, or their agents to the individuals or entities that reported a vulnerability to them.**

Some vulnerabilities will be reported to U.S. companies by people or entities outside of the U.S. and Canada. In some cases, the U.S. product manufacturers may need or want to engage with that person or entity (because, for instance, the initial bug report wasn't entirely clear, may not have contained all of the information needed to identify the full scope of the vulnerability, etc.). In the course of those discussions, it may be necessary for the U.S. product manufacturer to export to the vulnerability reporter materials falling within the scope of the intrusion software-related controls (such as 4E001.c technology). If, for example, a security researcher in Europe were to notify Google of a vulnerability in one of its products, it is in the best interest of users for the vulnerability to be addressed as quickly as possible. Such a bug reporter's goal is clearly to enhance user security, not exploit their vulnerability. It would be an odd and unfortunate result if Google were not able to communicate immediately with this bug reporter because doing so would result in the transfer of 4E001.c technology, thus requiring a long delay while an export license authorizing the transfer is processed. A license exception would authorize immediate exports and deemed exports without having to wait for approval from BIS. This requested license exception would be consistent with the President's directive that "private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." (See <http://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf>.)

- 4. BIS should develop a publicly available "flow chart" for analyzing its export controls relating to intrusion software.**

Although the license exceptions requested above would reduce the licensing burden relating to cybersecurity, the threshold question is whether a specific set of circumstances involves an export or deemed export of goods, software, or information controlled by ECCNs 4A005, 4D004, and 4E001.c.

The text of the various controls relating to intrusion software is a source of considerable confusion. BIS has provided FAQs for this proposed rule at <http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200> and has reiterated positions similar to the FAQ statements during public conference calls. After the proposed rule was first published in the Federal Register, it quickly became clear that BIS reads ECCNs 4A005, 4D004, and 4E001.c more narrowly than most security professionals analyzing the technical parameters of these controls. In its FAQs, BIS has stated that “[t]he proposed rule would not control the following: 1. Information on how to search for, discover or identify a vulnerability in a system, including vulnerability scanning; 2. Information about the vulnerability, including causes of the vulnerability.” (See FAQ 4 from <http://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>.) Although the conclusions themselves are encouraging, it is not obvious to us how the conclusions necessarily follow from or are supported by the control text itself. In some cases, as discussed in more detail in Section One regarding FAQ number 4 and 4E001.c, statements in the FAQs can actually conflict with the language of the controls themselves.

Google encourages BIS to develop a publicly available tool, such as a flow chart, for analyzing the text of the various controls relating to intrusion software. Such a tool would benefit all exporters and potential exporters in the security community. It would reduce uncertainty for all parties engaged in transactions that are subject to the EAR. Potential ambiguities would be reduced, decisions could be made more quickly, the need to contact BIS for advice would be reduced, and the possibility of inconsistent interpretations providing one party commercial advantages over others would be reduced.

- 5. To the extent that BIS intends to maintain distinct, restrictive licensing policies for rootkits and zero-day exploits, it should provide specific definitions for those terms.**

BIS has indicated that “there is a [license application review] policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.” If BIS does not adopt the license exceptions requested above, it should define these terms, which are susceptible to more than one potential interpretation. In fact, it is unclear that rootkits and zero-day exploits are even controlled under any of the new cybersecurity ECCNs for software. Based on our understanding of these terms, rootkits and zero-day exploits would represent examples of “intrusion software,” which is not controlled by ECCN 4D004. Either BIS has adopted an interpretation of the terms “rootkit” and “zero-day exploit” that is unfamiliar to us (and, we suspect, many others in the security community) or it has established a licensing policy for items that do not require an export license. However, Google would prefer that BIS adopt the license exceptions requested above,

which would obviate the need to enumerate licensing policies for such items or define these terms.

6. **BIS should amend these intrusion software-related controls at the next Wassenaar Arrangement meeting.**

Although Wassenaar Arrangement members may have adopted these cybersecurity controls because of concerns about privacy and human rights abuses, the actual controls they created are extremely broad in scope and not limited to what they probably hoped to capture. Accordingly, we request that BIS help change the Wassenaar Arrangement controls at its earliest opportunity in 2015. We encourage BIS to engage more closely with the broader security community to help narrow the technical parameters of export controls in a way that will not adversely affect the security of ordinary technology users across the world.

Thank you for your consideration. Please do not hesitate to contact us via email (neilmartin@google.com) or phone (650-253-1816) with any questions or comments regarding this submission.

Respectfully,

Neil Martin

Export Compliance Counsel
Google Inc.

PUBLIC SUBMISSION

As of: 7/29/15 3:30 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-ky5k
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0229

Frank McClain

Submitter Information

General Comment

See attached

Attachments

Frank McClain

Sharron Cook

From: Frank McClain <frank.mc.42@gmail.com>
Sent: Monday, July 20, 2015 12:02 PM
To: PublicComments
Subject: Comment Submission, Rule ID: BIS-2015-0011, RIN: 0694-AG49

Dear US Department of Commerce,

I am writing to express my concern regarding the above-referenced regulation, for the inclusion of “cybersecurity items” to the Commerce Control List (CCL) (Supplement No. 1 to part 774 of the Export Administration Regulations) as part of the Wassenaar Arrangement (WA). I am concerned that there will be negative ramifications from these new cyber regulations, with unforeseen and undesirable consequences to the Information Security community, industry, and our nation’s commercial well-being as a whole.

As with many others, I work in Information Security and have responsibilities to protect my employer’s electronic data, network, and computer assets. In order to best perform my duties, I have to be able not only to identify and respond to malicious actions (be they commodity or advanced malware, or active attacks of various nature), but to actively and in an ongoing way, test our network for resilience against such threats. Doing so requires us to be able to – without fear of legal repercussions – work with malware, exploit code, and associated frameworks to efficiently and effectively pressure-test our environment. In addition to “possessing” exploit code and the tools to run it against our environment, this also means the ability to research malware and exploit code, and reverse-engineer the same – both proactively (defense) and reactively (incident response).

I am aware of the arguments for control over these things, but as history continually shows, suppressing or prohibiting things considered to be used by criminals, does not in fact prevent criminals from possessing and utilizing them. All such legislation accomplishes is to prevent organizations and individuals from protecting themselves from criminals – the government cannot now, nor has it ever been able to, provide these protections to the degree necessary, especially from a cybersecurity perspective. Yes, we do need modern, effective, and appropriate regulations to help provide the government with the tools and ability to effectively capture and prosecute cybercriminals; but adding restrictions via WA, I fear, is not the answer – it will only serve to criminalize honest security researchers and businesses who are trying to do their best to serve their company, the industry, and our nation at large.

Respectfully,

Frank McClain

PUBLIC SUBMISSION

As of: 7/29/15 3:32 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-o8jx
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0230

FireEye Comments Wassenaar RIN 0694-AG49 final 7-29

Submitter Information

General Comment

See attached

Attachments

FireEye Comments Wassenaar RIN 0694-AG49 final 7-29

FireEye Comments regarding Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items RIN 0694-AG49

FireEye, Inc. ("FireEye") submits the following in response to Bureau of Industry's proposed rule implementing the Wassenaar Arrangement 2013 Plenary Agreements on Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015) ("the proposed rule").

As explained in detail in the comments filed by the Coalition for Responsible Cybersecurity, implementation of the proposed rule will have a detrimental impact on FireEye's ability to (i) sell its defensive cybersecurity products and services globally, and (ii) conduct cybersecurity vulnerability and threat research, a function that is inherently global.

Products and Services

As currently drafted, the proposed rule's overbroad language restricting the export of items designed for the "generation, operation, delivery or communication with" intrusion software and that perform either "extraction of data or information, from a computer or network-capable device, or modification of system or user data" or "modification of the standard execution path of a program or process" seemingly restricts the export of a majority of FireEye technology to include its enterprise, network and mobile products.

Many FireEye products allow users to execute in a secure virtual environment suspicious email attachments, binaries and web objects, mobile applications and malware against a range of browsers, plug-ins, applications, and operating environments. If an attack is identified, FireEye technology captures call back channels, dynamically creates blocking rules to prevent the malicious code from infecting the system and transmits this information back to the FireEye network. In order to accomplish this, FireEye technology must communicate with intrusion software, extract data from a computer or network-capable device and modify the standard execution path of a program or process. These defensive actions appear to fall squarely within the plain language of the proposed rule.

In addition, as currently drafted, the proposed rule restricts the use of penetration testing tools, root kits¹ and IP network communication surveillance system, equipment and components.² As these technologies are essential for understanding whether a system is vulnerable and/or already compromised and/or for building effective defenses, the proposed rule seemingly makes it very difficult, if not impossible, for FireEye to provide timely incident response, vulnerability and compromise assessments and managed security services to global customers.

Further, when an organization suffers a breach, time is of the essence. Incident responders must move quickly to respond to and contain a breach to mitigate adverse consequences. The delay and regulatory burden imposed by the proposed rule will ensure that prospective customers outside of the U.S. and Canada will give their business to non-U.S. based companies.

Research

As currently drafted, the proposed rule will likely undermine FireEye's efforts to share threat intelligence with its customers in near real time through its Distributed Threat Intelligence (DTI) cloud. The DTI cloud enables FireEye to anonymously exchange data on email, web and file based threats across its global customer base in near real time, ensuring that FireEye customers are protected against the most recent threats. Data exchanged through the DTI Cloud may include technical indicators, contextual information, malware command and control information, malware samples and other data that provides a clear picture of the malware infrastructure, capabilities and methodologies used by the attackers. The more data FireEye has to analyze and correlate, the better the protection FireEye will be able to provide its customers.

If FireEye is unable to share this threat intelligence in near-real time across borders because of licensing requirements, FireEye customers outside of the United States and Canada will not be protected from the most recent cyber threats, leaving them unnecessarily vulnerable to exploitation. This situation will provide cyber criminals with an advantage and strengthen the competitive position of non-U.S. based cybersecurity companies.

¹ FireEye is also concerned that the presumptive denial against the export of rootkits, an undefined term whose meaning is ambiguous, may restrict the export of FireEye's endpoint and forensic products.

² While BIS attempts to limit the restriction on IP communications surveillance tools to carrier class items, this phrase is undefined and its meaning is ambiguous.

As written, the proposed rule will also chill FireEye's threat and vulnerability research, which involves collaboration with individuals and organizations outside of the U.S., and foreign national employees in the U.S., on vulnerabilities and associated exploits and technical details, much of which is not publically available or intended for publication. If this type of activity requires a license, it will bring this valuable type of information sharing and collaboration to a halt.

The adverse consequences described above will be made worse by the policy of presumptive denial for export of zero-day exploit capabilities. While the proposed rule fails to define exactly what constitutes a zero-day exploit capability, the rule appears to restrict the ability of legitimate cybersecurity companies from effectively collaborating or sharing sufficient data to defend against them. In the past two years, FireEye discovered and developed defenses against 18 zero-day exploits. By seemingly restricting FireEye's ability to sell its products and services globally and preventing FireEye researchers from collaborating with global partners, the proposed rule will reduce FireEye's visibility into the rapidly evolving tactics and techniques of cyber attackers and likely reduce FireEye's unique ability to detect and prevent zero-day exploits.

In light of the potentially significant impact on FireEye and other U.S. based cybersecurity companies, FireEye respectfully requests that BIS substantially revise the proposed rule to address these points.

PUBLIC SUBMISSION

As of: 7/29/15 3:33 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-aolt
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0231

Financial Services Roundtable-BITS richard Foster 7-29

Submitter Information

General Comment

See attached

Attachments

Financial Services Roundtable-BITS richard Foster 7-29



July 20, 2015

By Electronic Filing (via Email: publiccomments@bis.doc.gov)

Catherine Wheeler
Director
Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave., N.W.
Washington, DC 20230

**Re: Proposed Rules for the Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items [RIN 0694-AG49]**

Dear Director Wheeler:

The Financial Services Roundtable/BITS (“FSR/BITS”)¹ welcomes the opportunity to provide comments to the Bureau of Industry and Security (the “Bureau”)

¹ About FSR and BITS: As advocates for a strong financial future™, FSR represents the largest integrated financial services companies providing banking, insurance, payment and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. FSR member companies provide fuel for America’s economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs. BITS is the technology policy division of FSR and addresses newly emerging threats and opportunities, particularly those related to cybersecurity, fraud reduction and critical infrastructure protection. Working with CEOs, CIOs, heads of IT Risk and other senior members of member companies, BITS identifies key issues at the intersection of financial services, technology and commerce and facilitates collaboration to improve the ecommerce environment for member companies and their customers through the development of policies and practices.

on its proposed rules for implementing the Wassenaar Arrangement (“WA”) 2013 Plenary Agreements as they pertain to Intrusion and Surveillance Items (“Proposed Rules”).

Like the Bureau, FSR/BITS members, which include many of the largest financial institutions in the United States, are concerned about the cybersecurity risks that are posed by the offensive use of the items described in this proposed rulemaking, namely:

- “systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software”;
- “software specially designed or modified for the development or production of such systems, equipment or components”;
- “software specially designed for the generation, operation or delivery of, or communication with, intrusion software”;
- “technology required for the development of intrusion software”;
- “Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefore, and development and production software and technology therefor.”²

In the hands of those with malicious intent, these items have the potential to pose some of the gravest cyber risks this and other nations face.

Nonetheless, FSR/BITS’s principal concern arises from the fact that the Proposed Rules draw no distinctions between the offensive and malicious use of the proposed items and use for purely beneficial and protective purposes. While the lack of such distinctions

² Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28853 (May 20, 2015).

is common in other dual-use arenas, in the cybersecurity context it poses significant risks to our nation's national security, particularly to our nation's critical infrastructure entities that have an international footprint or employ non-U.S. citizens.³ More specifically, as Cheri McGuire, the past Acting Director of the Department of Homeland Security National Cyber Security Division and US-CERT and now cybersecurity expert and executive at Symantec, recently stated, “[t]he proposed rule would severely damage legitimate vulnerability research and security testing worldwide, and thus undermine our ability to protect our own networks and to innovate cybersecurity products and services. The end result is that our customers – businesses, governments and consumers – would be less secure and at greater risk.”⁴

Additionally, as further described below, the Proposed Rules, if promulgated as drafted, will place FSR/BITS's members, and the Bureau itself, arguably in conflict with other federal statutes, federal agency regulations, and other cybersecurity goals and statutory and regulatory requirements and guidance, including, but not limited to, those set forth in the Federal Information Security Management Act (“FISMA”) and the Gramm-Leach-Bliley Act, and those provided by another sub-agency of the Department of Commerce, the National Institute of Standards and Technology (“NIST”). For this reason, we believe the Proposed Rules' approach should be reconsidered, and that much greater inter-agency coordination must be undertaken, including coordination with federal, state, and local law enforcement as well as with financial sector and other sector regulatory agencies.

³ See 15 C.F.R. § 734.2(b)(1) (2012) (“‘Export’ means an actual shipment or transmission of items subject to the EAR out of the United States, or release of technology or software subject to the EAR to a foreign national in the United States, as described in paragraph (b)(2)(ii) of this section.”); *id.* § 734.2(b)(2)(ii) (“Such release is deemed to be an export to the home country or countries of the foreign national. This deemed export rule does not apply to persons lawfully admitted for permanent residence in the United States . . .”).

⁴ Cheri F. McGuire, “U.S. Commerce Department Controversial Cybersecurity Rule Will Weaken Security Industry and Worldwide Protection,” Symantec Official Blog (July 14, 2015), *available at* <http://www.symantec.com/connect/blogs/us-commerce-department-controversial-cybersecurity-rule-will-weaken-security-industry-and-worl>.

Alternatively, FSR/BITS urges the Bureau to modify the Proposed Rules substantially to explicitly exempt from the restrictions and licensing scheme that usage which is for defensive purposes.

In the remainder of these comments, we identify the reasoning and support for these suggestions, and, in particular, the potential risks to financial institutions and other private sector companies and individuals, if the Proposed Rules are implemented without modifications to their features that could lead to an unintended inability to protect our nation's critical infrastructure and a series of potential statutory and regulatory conflicts.

I. The Regulations Would Harm National Security.

As an initial matter, the Proposed Rules would seriously and substantially diminish industry's ability to effectively run day-to-day cybersecurity assurance programs. A major component of these programs involves tasking vulnerability assessment teams ("Red Teams")⁵ using company personnel and internally developed "intrusion software" to assess the security of network devices and applications. The ability to perform this activity unrestricted across global boundaries, but within the confines of a single firm, must not be hampered. Yet, if the Proposed Rules are promulgated, Global financial service enterprises deploying these teams would run afoul of the proposed "intrusion software" licensing regime. The Proposed Rules would affect use of "[s]ystems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software includ[ing] network penetration testing products that use intrusion software to identify

⁵ A Red Team is a "group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment." NIST, "Glossary of Key Information Security Terms," NIST IR 7298 Revision 2, p.156 (May 2013), *available at* <http://dx.doi.org/10.6028/NIST.IR.7298r2>.

vulnerabilities of computers and network-capable devices.”⁶ As proposed, the definition of “intrusion software,” would include software designed to avoid detection “monitoring tools,” defeat “protective countermeasures,” extract or modify data, or modify the “standard execution path.”⁷ Such a broad definition would encompass any and all effective penetration testing software, which is designed to circumvent in-place defensive controls, software, etc., and requires command and control of the implants or exploits in order to safely and effectively conduct defensive testing activities. Such language also suggests that licenses will be required every time a company develops its own software or purchases, for example, the commercial Metasploit framework and wishes to export these tools. While the Bureau seeks to maintain U.S. export controls on items included in the WA’s control list, the Bureau is probably not intending to make it more difficult for businesses to defend themselves. Yet the Proposed Regulations, applied as written, will have exactly these kinds of untoward effects because the Proposed Rules would require export control decisions for activities that are designed to strengthen cyber-defenses worldwide.

Subjecting these tools, and each individual upgrade, update, hotfix, and patch thereto, to the Export Administration Regulations’ (“EAR”) export license requirements will very significantly increase the volume of license applications required of any cybersecurity assurance program. In addition, the delay contemplated by the EAR license application process is, simply put, a product of an era whose assumptions about technology no longer hold true, especially given the speed, sophistication, and tirelessness of today’s hacking community. Delays of even hours in a company’s ability to detect and respond to a zero-day cyber attack can greatly limit the effectiveness of mitigating such an attack, and can lead to a cascade of harms inflicted not only on the targeted entity, but also interconnected third parties and the customers that have entrusted

⁶ Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854.

⁷ *Id.* at 28858.

their data to the entity. Indeed, in order to preserve any level of effectiveness against the constantly evolving universe of software exploits, cybersecurity tools, such as reconnaissance tools, exploitation toolkits, password crackers, vulnerability scanners, network scanners and sniffers, and hardware devices supporting the aforementioned activity, must be available and ready to use in real-time. Delays in the ability to keep these cybersecurity tools current will likely render them ineffective.

II. The Manner in Which the Proposed Rules Conflict with National Policy and Potentially with Existing Statutes, Regulations, and Guidance.

Under the Proposed Rules, companies would, for at least significant stretches at a time, lose the ability to utilize the important tools described above in combating cyber attacks. This loss is not only harmful, but also plainly contradicts federal policy. Indeed, it even has the potential to conflict with the requirements of other federal statutes, regulations and guidance, including FISMA and corresponding requirements developed and published by the NIST. For example, according to NIST Special Publication 800-53 Revision 4, CA-8, when a federal organization or contractor operating on its behalf operates a “high control baseline” information system, it **must** conduct penetration testing pursuant to FISMA.⁸ In its description of the penetration testing requirement,

⁸ The “Computer standards program” section of FISMA, 15 U.S.C. § 278g-3, directs the Department of Commerce through NIST to develop standards, guidelines, and minimum requirements “for information systems used or operated by an agency or by a contractor of an agency” *See* 15 U.S.C. § 278g-3(a)(2). After developing such standards, NIST was directed to submit them to the Secretary of Commerce for approval. Pursuant to FISMA’s directive, the NIST’s “Minimum Security Requirements for Federal Information and Information Systems” was approved in March 2006. *See* NIST, “Minimum Security Requirements for Federal Information and Information Systems,” FIPS 200 (Mar. 2006), *available at* <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>. These requirements state:

“[o]rganizations must meet the minimum security requirements in this standard by selecting the appropriate security controls and assurance requirements as described in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems The selected set of security controls must include one of three, appropriately tailored security control baselines from NIST Special Publication 800-53 that are associated with the designated impact levels of the organizational information systems as determined during the security categorization process.

...

NIST SP 800-53 Revision 4, CA-8, states that “[s]uch testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (*e.g.*, time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies.”⁹

Additionally, in early 2013, President Obama signed Executive Order 13636, titled “Improving Critical Infrastructure Cybersecurity.” Among other things, the President ordered the Secretary of Commerce to direct NIST to develop a Cybersecurity Framework of cyber best practices and methodologies in conjunction with other stakeholders, including owners and operators of critical infrastructure entities.¹⁰ In February 2014, NIST released Version 1.0 of this Cybersecurity Framework.¹¹ In the Framework, NIST cites to NIST SP 800-53, CA-8 – the penetration testing recommendation – and suggests under subcategory ID.RA-1 that “Asset vulnerabilities [be] identified and documented.”¹² Together, this indicates an endorsement of penetration testing as a cybersecurity tool, a tool that, as mentioned, would necessarily circumvent in-place defenses, and, thus, qualify for export control restriction.

“For *high-impact* information systems, organizations must, as a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST Special Publication 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.”

Id. at 4. As mentioned above, NIST SP 800-53 states that penetration testing is a “high baseline control” requirement. *See* NIST, “Security and Privacy Controls for Federal Information Systems and Organizations,” SP 800-53 Revision 4, Appendix D, p.D-17 (Apr. 30, 2013), *available at* <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.

⁹ NIST, SP 800-53 Revision 4 at Appendix F-CA, p.F-62.

¹⁰ *See* Exec. Order No. 13636, 78 Fed. Reg. 11739, 11740-41 (2013).

¹¹ *See* NIST, “Framework for Improving Critical Infrastructure Cybersecurity” (Feb. 2014), *available at* <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

¹² *See id.* at 22

Finally, NIST also issued SP 800-115, titled “Technical Guide to Information Security Testing and Assessment.” Like the other NIST guidance, SP 800-115 recommends penetration testing, calling it “invaluable” and stating that it is “useful for determining:

- How well the system tolerates real world-style attack patterns
- The likely level of sophistication an attacker needs to successfully compromise the system
- Additional countermeasures that could mitigate threats against the system
- Defenders’ ability to detect attacks and respond appropriately.”¹³

The publication further states, “Penetration testing is important for determining the vulnerability of an organization’s network and the level of damage that can occur if the network is compromised. [. . .] A well-designed program of regularly scheduled network and vulnerability scanning, interspersed with periodic penetration testing, can help prevent many types of attacks and reduce the potential impact of successful ones.”¹⁴

In addition to generating conflicts with the aforementioned mandates and policy guidance, the Proposed Rules also have the potential to conflict with federal statutes and guidance specific to our sector: the financial services sector. Under the Gramm-Leach-Bliley Act’s “Safeguards” provisions, 12 U.S.C. §§ 6801, 6805; *see also id.* § 1831p-1; *id.* § 3301 *et seq.*, the “prudential” regulators of the financial services industry – among other regulatory agencies, the Board of Governors of the Federal Reserve System (“FRB”), the Federal Deposit Insurance Corporation (“FDIC”), and the Office of the Comptroller of the Currency (“OCC”) – are directed to establish a uniform set of

¹³ *See* NIST, “Technical Guidance to Information Security Testing and Assessment,” SP 800-115, Section 5.2, p.5-2 (2008), *available at* <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>.

¹⁴ *See id.* at Section 5.2.2, p.5-6.

information security standards applicable to those segments of the financial services sector that they regulate. Together, they developed and released the “Interagency Guidelines Establishing Information Security Standards,”¹⁵ the Federal Financial Institutions Examination Council (“FFIEC”) IT Examination Handbooks, and the most recently released FFIEC Cybersecurity Assessment Tool. According to the Interagency Guidelines, each financial institution must “identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems,” and to do so, each financial institution must “[r]egularly test the key controls, systems and procedures of the information security program.”¹⁶

Both the FFIEC IT Examination Handbook series and the FFIEC Cybersecurity Assessment Tool provide more detail about these mandates. In the “Information Security” IT Examination Handbook, the regulators state that, as part of an information security program, they expect financial institutions to conduct independent tests of their software that include, among other things, penetration tests.¹⁷ Citing this provision of the Information Security IT Examination Handbook, the FFIEC Cybersecurity Assessment Tool goes further, indicating that penetration testing is a cybersecurity program’s baseline maturity requirement.¹⁸ According to the Tool, baseline maturity is “characterized by minimum expectations required by law and regulations or recommended in supervisory guidance.”¹⁹ Moreover, the OCC stated that it will be gradually implementing the

¹⁵ The “Interagency Guidelines Establishing Information Security Standards” was jointly issued by the FRB, the FDIC, the OCC, and the Office of Thrift Supervision (“OTS”). This jointly issued guidance is promulgated under 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS).

¹⁶ 12 C.F.R. Part 225, app. F.

¹⁷ FFIEC, “‘Information Security’ IT Examination Handbook,” p.81 (July 2006), *available at* http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf.

¹⁸ FFIEC, “Cybersecurity Assessment Tool,” p.41 (2015), *available at* https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

¹⁹ *Id.* at 7.

FFIEC's Tool during the course of bank examinations.²⁰ This Tool, as described by the OCC, will "help[] banks and examiners determine a bank's inherent risk profile and level of cybersecurity preparedness,"²¹ and "the results may be reviewed to determine whether the bank's cybersecurity maturity levels align with the bank's inherent risk profile."²² By hampering financial institutions' ability to detect and respond to potential cyber attacks, the Proposed Rules thus pose critical obstacles to achieving the prudential regulators' regulatory goals, placing FSR/BITS members subject to FRB, FDIC, and OCC regulation in conflict with their primary regulators' directives.

Other agencies within the government stress the importance of speed in response to cyber attacks, heightening the conflicts posed by the Proposed Rules. The U.S. Department of Justice's ("DOJ") guidance on cybersecurity states that "[d]uring an intrusion, an organization's management and personnel should be focused on containing the intrusion, mitigating the harm, and collecting and preserving the vital information that will help them assess the nature and scope of the damage and the potential source of the threat."²³ The Federal Trade Commission ("FTC") has issued similar admonishments.²⁴

None of these federal agency approaches, including even the Department of Commerce's own, contemplates potentially weeks or even possibly months-long delays in the licensing of defensive uses of systems, equipment, or components that may be necessary to identify and prevent cyber attacks, or limit the damage of an attack once one has begun. To the contrary, particularly in the case of zero-day attacks, in which a

²⁰ See OCC, "FFIEC Cybersecurity Assessment Tool," Bulletin 2015-31 (June 30, 2015), available at <http://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-31.html>.

²¹ *Id.*

²² *Id.*

²³ See DOJ, "Best Practices for Victim Response and Reporting of Cyber Incidents" (May 2015), available at <http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf>.

²⁴ See FTC, "Start with Security: A Guide for Business" (June 30, 2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>.

vulnerability could not have been reasonably known ahead of time, “advance planning” to obtain licensure may be impossible. Yet, with only the most limited form of emergency licensure, the Proposed Rules will impose significant burdens on FSR/BITS members’ ability to take effective defensive action.

III. The Risks to Cybersecurity Noted Above are Far From Theoretical.

FSR/BITS contends that the above concerns are far from theoretical. According to the Bureau’s own statistics, in FY 2014 it took an average of 23 days to review an EAR license application.²⁵ The Proposed Rules, however, allow the Bureau up to 90 days to review an application after it is registered.²⁶ While it is directed to register license applications “promptly” upon receipt,²⁷ several activities do not count against the 90-day window.²⁸ For example, the Bureau may consult with other U.S. departments and agencies regarding licenses it receives.²⁹ The agency whose comments are sought then has up to 30 days to provide the Bureau with a recommendation to either approve or deny the license application.³⁰ This period is excluded from the Bureau’s 90-day limit.

Emergency processing is available upon request, and “[the Bureau] will expedite its evaluation, and attempt to expedite the evaluations of other government agencies, of a license application when, in its sole judgment, the circumstances justify emergency processing.”³¹ Applicants must call the Outreach and Educational Services Division of the Office of Exporter Services to request expedited review.³² Presumably, however,

²⁵ Bureau, Annual Report to the Congress for Fiscal Year 2014, available at https://www.bis.doc.gov/index.php/forms-documents/doc_download/1183-bis-annual-report-2014.

²⁶ 15 C.F.R. § 750.4(a) (2012).

²⁷ *Id.*

²⁸ *See id.* § 750.4(b).

²⁹ *Id.* § 750.3(a).

³⁰ *Id.* § 750.4(d)(2).

³¹ *Id.* § 748.4(h).

³² *Id.*

whether emergency review is granted would be matters entrusted to the Bureau's discretion, providing only limited judicial review in the event of denial of expedition.

The application waiting period is in addition to the process for completing an application.³³ Under the Proposed Rules, the listed items may not be anticipatorily exported without a license. License applications must be filed electronically via the Bureau's Simplified Network Application Processing System ("SNAP-R"), unless the Bureau authorizes submission in paper form.³⁴ Only a person in the United States would be eligible to apply for a license to export items from the United States.³⁵

As Ms. McGuire of Symantec has stated: "Asking a multinational corporation who is at risk of a cyber attack to wait months for a license to be able to test its network defenses, or to receive the latest protections because its security provider is hampered from communicating across borders, is downright dangerous."³⁶ Penetration testing software requires periodic updates to effectively combat potential threats. It is often the case that, by the time the updated components reach their destination, the components can already be partially out of date due to the speed with which the technology evolves.

³³ The first step in the process for obtaining a license involves registering on SNAP-R. 15 C.F.R. § 748.7(b). While a company is able to fill out the application itself, *id.* at Supp. No. 1, the application asks for a variety of information, including the name of a contact person, the type of license requested, the name of the applicant, the purchaser of the goods, the end-user of the goods, the end-use, the quantity of goods shipped, and their unit price. An exporter of the command and delivery platforms for generating, operating, delivering, and communicating with "intrusion software" would also be required to supply the information detailed in 15 C.F.R. § 748, Supp. No. 2(z). *See* Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858. The Proposed Rule would not control the "intrusion software" itself, but, among other things, Supp. No. 2(z) requires the applicant to submit the following in a letter of explanation: (1) whether the cybersecurity item has encryption or other information security information; and (2) whether the cybersecurity item has previously been classified under the amendments made to the EAR in May 2015. If the cybersecurity item for which the license is sought has not been classified under the currently amended regulation, the applicant must supply additional technical information. *See* 15 C.F.R. § 748, Supp. No. 2(z).

³⁴ 15 C.F.R. § 748.1(d).

³⁵ *Id.* § 748.4(a).

³⁶ McGuire, *supra* note 4.

Even if the Bureau were to approve a license application within 23 days, as is the current average, the licensed software product could be, in effect, obsolete or useless.

Moreover, there is a risk that cybersecurity efforts could be weakened by the need periodically to re-apply for licenses. Generally speaking, licenses to be issued under the regulations will have a 24-month validity period,³⁷ while emergency licenses would expire “no later than the last day of the calendar month following the month in which the emergency license is issued.”³⁸ Applicants may request validity periods in excess of 24 months for non-emergency licenses, but these requests “generally will not be granted.”³⁹ Under the existing process to which the proposed list items will be subject, the Bureau will consider granting a validity period in excess of 24 months if “extenuating circumstances” warrant.⁴⁰ Yet the circumstances for extended periods appear limited; *i.e.*, the Bureau will generally grant an extended validity period where “the transaction is related to a multi-year project, when production lead time will not permit an export or re-export during the original validity period of the license, when an unforeseen emergency prevents shipment within the 24-month validity of the license, or for other similar circumstances.”⁴¹ By utilizing the existing license framework, the Proposed Rules would “authorize[] only a specific transaction, or series of transactions, as described in the license application and any supporting documents.”⁴² Generally, this means that licenses cannot be materially altered after approval.⁴³

³⁷ See 15 C.F.R. § 750.7(g).

³⁸ *Id.*

³⁹ *Id.* § 750.7(g)(1).

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.* § 750.7(a).

⁴³ *Id.* §§ 750.7(c), 748, Supp. No. 1. In addition, under the Proposed Rules, exporters of command and delivery platforms for generating, operating, delivering, and communicating with “intrusion software” would have to follow the procedures discussed above because “no license exceptions would be available for these items, except certain provisions of License Exception GOV.” Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854. This is

IV. Conclusion

In light of the above, FSR/BITS suggests that the Bureau should hold the Proposed Rules in abeyance and consider undertaking additional consultations with other federal agencies, including the FRB, OCC, FDIC, FTC, and DOJ, as well as related agencies with portfolios for national security, to better assess whether fulfillment of the United States' determination to implement the WA's recommendations through amendments to the EAR licensing requirements, as proposed, is the most effective way to minimize cyber risk.

While the Bureau notes that “the Departments of Defense and State, as well as other agencies have been discussing the best way to add these items . . . to the Commerce Control List,”⁴⁴ FSR/BITS remains concerned that adequate input from law enforcement, and bank and other financial institution regulators has not been obtained in a way that

especially problematic because an item possessing both encryption technology and the ability to communicate and deliver “intrusion software” would lose the ability to use License Exception ENC. While “[the Bureau] anticipates licensing broad authorizations to certain types of end users and destinations,” *id.* at 28855, these end users and destinations are not defined or in any way specified in the proposed regulations. Applications to export the command and delivery platforms for generating, operating, delivering, and communicating with “intrusion software” will face potentially even greater scrutiny than those for exporting encryption software where licenses for the latter are required. License applications for exporting encryption software are to be reviewed “on a case-by-case basis by [the Bureau], in conjunction with other agencies, to determine whether the export or re-export is consistent with U.S. national security and foreign policy interests.” 15 C.F.R. § 742.15(b). In the Proposed Rules, command and delivery platforms for “intrusion software” were added to 15 C.F.R. § 774 to promote regional stability, among other reasons. Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854. The Bureau has relatedly proposed a new section to 15 C.F.R. § 742.6(b) that increases the scrutiny of cybersecurity items controlled to promote such stability. Applications for exporting such items will be reviewed “favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1.” Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28857-58; *see* 15 C.F.R. § 740, Supp. No. 1 for a list of countries that fall into these groups. Even though the applications will be looked on favorably here, however, the Bureau will review each application “on a case-by-case basis to determine whether the transaction is contrary to national security or foreign policy interests of the U.S. . . . except that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.” Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28858. These are items that may be most important to export to address genuine defensive issues, however.

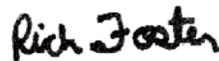
⁴⁴ Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. at 28854.

ensures that FSR/BITS members and those in related industries are not unduly hamstrung in their efforts to fight and contain cyber attacks, and that, at a minimum, FSR/BITS members are not subjected to conflicting regulation. The reality is that if a criminal organization is resolute on committing a cyber attack, it will be violating many laws, both in the United States and abroad, and the addition of one more set of laws (*i.e.*, the export regulations) will not necessarily deter cyber-crime. At the same time, the Proposed Rules will, if promulgated as written, potentially hamper company efforts to prevent and mitigate the harm from cyber-crime through defensive use of technology. We urge the Bureau, specifically, to determine whether a different approach that exempts defensive uses of the listed items would better serve its purpose without harming national security.

* * *

We thank the Bureau for considering these comments and respectfully urge the Bureau to reconsider the Proposed Rules in light of the concerns noted above. If you have any questions, please feel free to contact me at (202) 589-2424 or Josh Magri at either (202) 589-1927 or Josh.Magri@FSRoundtable.org.

Respectfully submitted,



Richard Foster
Senior Vice President and Senior Counsel
for Regulatory and Legal Affairs
Financial Services Roundtable
600 13th Street, N.W.
Suite 400
Washington, D.C. 20005

PUBLIC SUBMISSION

As of: 7/29/15 3:34 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-glxh
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0232

Final Group Letter_July 20 2015 7-29

Submitter Information

General Comment

See attached

Attachments

Final Group Letter_July 20 2015 7-29

July 20, 2015

Via email to publiccomments@bis.doc.gov

Kevin J. Wolf
Assistant Secretary for Export Administration
Regulatory Policy Division, Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC 20230

Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (Docket No. 150304218-5218-01; RIN 0694-AG49)

Dear Assistant Secretary Wolf:

Our organizations, which represent nearly every sector of the U.S. economy, welcome the opportunity to comment on the Bureau of Industry and Security's (BIS') proposed rule, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, released in the *Federal Register* on May 20, 2015.¹ Cybersecurity is a top policy priority of our members. The goals of the Wassenaar Arrangement (WA) are constructive, and our organizations appreciate BIS' attention to combating the proliferation of malicious and weaponized software. However, we have genuine concerns that if the proposed rule were to go into effect without substantial changes, it could harm rather than improve U.S. cybersecurity.

We do not attempt to answer each question in the May 20 notice seeking comment. However, we try to explain why our organizations believe that BIS' proposed rule is too expansive and the license requirements are overly strict. Our associations recommend that BIS narrows the breadth of cyber items that would be controlled and builds more flexibility into the rule's conditions. We believe that the United States can meet the terms of the WA without sacrificing the prudence needed to make the proposal.

Businesses would likely need to submit hundreds, perhaps thousands, of additional license applications under the requirements of BIS' proposed rule.

The number of new export licenses that U.S. companies would have to request from BIS could be staggering—ranging from hundreds to perhaps thousands—depending on the number of products in their software portfolios. Factors influencing license applications include the volume of third-party software and services that companies use in their own operations, the number of offices that they have outside of the United States and Canada (which is exempt from the proposed rule), and the number of engineers that companies employ or are in contact with who are not American citizens. Also, the burden of determining what activities require licensing would be significant for businesses' software development cycles, code in transient states, and

¹ www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

email communications housing information—all of which may be ostensibly covered under BIS’ proposed rule.

Making matters more complicated, the bureau’s proposed rule states that “when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled cybersecurity functionality.”² The bureau should reconsider the mandate for applicants to hand over their source code. This is particularly important at a time when U.S. officials and industry are urging foreign governments not to compel vendors to turn over intellectual property, such as source code and other sensitive corporate data.

The rule would have negative effects on businesses’ legitimate vulnerability research, audits, testing, and screening. Businesses’ ability to protect their (or a client’s) information systems would be thrown into question.

“Intrusion software”-related items as listed under the Wassenaar Agreement (WA) and proposed for regulation by BIS would severely restrict security vulnerability improvements and R&D undertaken by U.S. companies, academia, nonprofits, and individuals. The proposed rule would affect entities that create or operate intrusion software and any information system that “communicates with” such intrusion software.

To be sure, BIS argues that intrusion software, malware, and exploits themselves would not be controlled. For instance, in an FAQ supplement to the proposed rule, the bureau tries to distinguish between “intrusion software,” which is not controlled per se, and items such as “command and control and delivery platforms,” which would be controlled by U.S. export officials:

[T]he proposed rule would not control any “intrusion software,” which may also be referred to as malware or exploits. The Category 4 control entries would control the command and delivery platforms for generating, operating, delivering, and communicating with “intrusion software.” It would also control the technology for developing “intrusion software,” but it does not control the “intrusion software” itself. Thus, transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware would not be included in the new control list entries and would not require a license under the proposed rule.³

What is especially challenging for our organizations to understand is that BIS, in order to comply with WA, would require businesses to make nuanced distinctions between various forms of intrusion software and the technical data for developing exploits. Such differentiations are nearly impossible to make in practice.

In addition, BIS’ rule proposal would significantly restrict testing and research into cyber vulnerabilities and exploits connected to valuable internal business activities (“intra-company transfers or internal use”),⁴ which are designed to strengthen their cyber defenses worldwide.

² See, for example, FAQ No. 7 via www.bis.doc.gov/index.php/policy-guidance/faqs.

³ See FAQs Nos. 1 and 3.

⁴ See FAQ No. 17.

Such limitations are troublesome to our associations. On the one hand, business initiatives meant to protect their information systems should be aided and encouraged, not restrained. On the other hand, delays in approvals for license applications would almost certainly leave critical data systems much less protected and subject to increased cyberattacks or breaches by malicious actors.

The proposed rule would spur the publication of unpatched vulnerabilities and constrain businesses’ ability to defend their information systems.

The apparent goal of BIS’ proposal is to reduce the production and sale of malicious and weaponized software. Strangely, the BIS proposal could have the exact opposite effect. The model that many in industry have for managing vulnerabilities is based on communicating unpublished vulnerability information to companies that can fix software problems before weaknesses are exploited. However, the proposed rule suggests forcing companies to publish vulnerabilities first—or otherwise making them publicly available—in order to conduct necessary research on exploits and transfer information in compliance with export rules.⁵

Revealing vulnerabilities before patches can be built is very disconcerting. The proposed rule would stimulate the publication of vulnerability information for which no known patches, fixes, or mitigations may be available. Instead, our organizations believe that BIS should be encouraging the discrete transfer of information about previously unknown vulnerabilities to the developers of the technology affected.

Also, the bureau’s proposed regulation would impose significant constraints on the ability of multinational corporations to take cyber self-defense actions, which private entities have an inherent right to. Companies’ vulnerability assessment personnel—aka red teams—use “intrusion software” to identify and track vulnerabilities in network devices and applications. Our organizations believe that the ability of companies to perform this activity across global boundaries, but within the confines of a single firm, must not be curtailed.

The BIS’ proposal would advance “a policy of presumptive denial” for zero-day and rootkit capabilities, e.g., “product or system” or “delivery tool” (p. 28855).⁶ Presumptive denial would greatly restrict businesses’ abilities to share threat information and counter some of the most dangerous cyber vulnerabilities and exploits.

Detailed technical data on the origins of a previously unknown vulnerability—a zero-day—is also the technology that enables bad actors to exploit weaknesses in a computer system. Potentially high-risk vulnerabilities are the exact type of cyber weaknesses that companies want to find during their internal penetration testing and exercises. Such vulnerabilities are given top priority by companies to examine and mitigate or eliminate fully to render exploits useless.

Zero-days are among the most dangerous of all cyber vulnerabilities and associated exploits, and they are unknown to the broader cyber stakeholder community. Responsible companies take vigorous steps to ensure that this sensitive information never leaks to the public,

⁵ See FAQ No. 5, among others.

⁶ See, too, FAQ No. 22.

which conflicts with BIS' push to make cyber technology or software "publicly available."⁷ Zero-day exploits have been known to cripple companies and their customers. The business community needs to be able to disseminate vulnerabilities and technical details to knowledgeable experts in their companies and trusted industry partners. Sometimes the experts will not be American or Canadian citizens.

If BIS automatically denies licenses for cyber items that have zero-day exploits, the policy could dramatically hinder a company from fixing the vulnerability, thus putting itself and its customers in jeopardy. We believe that BIS does not seek such an outcome from the proposed rule.

On a more granular level, BIS' proposed export control regime would impose severe limitations on currently lawful and smart business activities, including the following:

- The development, operation, and functionality of automated security vulnerability identification and reporting tools, application program interfaces (APIs), or backend systems that companies build into their own software products to defend their information systems.
- The speed of deployment of security patches for products impacted by intrusion software and related exploits (e.g., POODLE).
- Vendors that companies use for collecting and analyzing cybersecurity information and intelligence.
- Email accounts set up by companies to specifically receive security threat and vulnerability information from the general public.
- Software products that companies sell to provide situational awareness concerning cyber threats to their own computer systems as well as those of their customers.
- The work of security vulnerability researchers at U.S. and international universities that share threat information directly with U.S. companies (e.g., zero-day vulnerabilities) over email.
- Bug bounties and hackathon events, which are created to identify security exploits and then share that information back with the affected companies as quickly as possible.
- The types of audits that companies would be allowed to perform on third-party vendor systems and whether bugs could be reported back to them directly when discovered.
- The sharing of information between a single company's employees if someone within the United States shares technical data about security threats with a person who is not a citizen of the United States or Canada.

⁷ See, for example, FAQ No. 28.

- Threat data that companies and researchers need to share in timely ways within public-private partnerships (e.g., sector-coordinating councils and information-sharing and analysis organizations).
- Information sharing linked to government contracts and protected programs. First, information that is shared with the U.S. government voluntarily (e.g., US-CERT) or as required under contracts (e.g., FISMA and FedRAMP) could be thrown into question, which would benefit neither the government nor the private contractor.

Second, at the time of this writing, legislation is being considered in Congress for spurring the voluntary sharing of cyber threat information among multiple businesses and federal entities to improve cybersecurity. The bureau’s proposed rule could undermine, albeit unintentionally, the sharing processes and safeguards (e.g., legal liability and regulations) afforded to U.S. companies under the legislation.

Big picture: Our organizations believe that BIS’ proposed rule is much too broad and the license requirements are unreasonably stringent. The bureau should consider both narrowing the scope of the proposed rule (in terms of cyber items that would be swept up and controlled) and building more flexibility into the rule’s requirements. We believe that the United States can thoughtfully meet the terms of the WA without sacrificing the discretion required to make the proposal achievable, especially as it relates to safeguarding legitimate enterprise cyber risk management activities.

Aside from offering the perspectives above for BIS’ consideration, our organizations have further topics and questions that we respectfully ask bureau officials to please clarify:

- The proposed rule targets “technology required for the development of intrusion software” (p. 28853). Generally, to develop intrusion software for the Windows environment, you need tools such as Wintel-compatible hardware and a Windows operating system. Most companies use such tools for all their internal application development. However, an initial reading of the BIS notice could lead entities to believe that Wintel-compatible hardware and Windows operating systems would be controlled since they are required for development of intrusion software, which is not BIS’ intent.

Therefore, shouldn’t the proposed rule’s wording be changed to something closer to “technology required *solely* for the development of intrusion software and not used for *legitimate* purposes” (italics added for emphasis)? The WA goal, which BIS and our organizations share, is to dramatically limit the actions of bad actors while enabling businesses to conduct rightful security activities.

- Some interpret the proposed rule’s language—“systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software” (p.

28854). The word “specially” is seemingly meant to differentiate legitimate from illegitimate uses of intrusion software, but it is far from clear.

We suggest that BIS make it clear it is not talking about systems, equipment, components, and software that have legitimate purposes, even if bad actors use the same items for the purpose of invading information systems.

- BIS should better define what “communication with intrusion software” (p. 28854) means. At this point in the rule development process, it appears that nearly every software tool used to fight malicious software and intrusion software would be included. This cannot be the outcome that BIS is seeking.
- Most companies utilize some type of packet analyzer (aka packet sniffer) to monitor and capture digital traffic passing over a network so that technicians can identify malicious code. In 2013, WA agreed to add the following to their list of dual-use goods, including “Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor” (p. 28854).

Does the inclusion of IP network communications, etc., mean that companies would no longer be able to move their monitoring equipment and software from location to location in their networks to fight bad actors? Requiring government’s approval for such smart and basic cybersecurity practices strikes us as logistically unfeasible and detrimental to enterprise security.

- Most large multinational firms regularly undergo penetration testing to spot and remediate vulnerabilities in their computer systems. The proposed rule would impact “[s]ystems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices” (p. 28854).

Such language suggests that companies would have to gain licenses for nearly every test that they conduct outside the United States, since they would be moving computer equipment and software. While BIS is supposed to maintain U.S. export controls on items included on the WA’s control list, the bureau is probably not intending to make it *more* difficult for businesses to defend themselves, which is what this clause suggests.

Our associations are committed to working with BIS officials and other policymakers to strengthen U.S. cybersecurity by advancing smart, effective, and efficient policies at home and globally. We appreciate the opportunity to comment on the bureau’s proposed rule. Our members particularly appreciate the constructive outreach that they have had with BIS officials—Catherine “Randy” Wheeler, Aaron Amundson, and Anita Zinzuvadia. We urge the BIS not to rush to finalize this proposed rule, which is unworkable in its current form. The

proposed regime would tie the hands of businesses' legitimate cybersecurity activities while malicious actors simply disregard compliance.

Sincerely,

Alliance of Automobile Manufacturers
American Petroleum Institute (API)
Computer & Communications Industry Association (CCIA)
Information Technology Industry Council (ITI)
Internet Association
Financial Services Roundtable/BITS
National Foreign Trade Council
TechNet
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce

PUBLIC SUBMISSION

As of: 7/29/15 3:36 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-2tek
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0233

Cisco Eric Wenger

Submitter Information

General Comment

See attached

Attachments

Cisco Eric Wenger



Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

July 20, 2015

Via email to publiccomments@bis.doc.gov

Kevin J. Wolf
Assistant Secretary for Export Administration
Regulatory Policy Division, Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC 20230

**Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation:
Intrusion and Surveillance Items (Docket No. 150304218-5218-01; RIN 0694-AG49)**

Dear Assistant Secretary Wolf:

I am writing today on behalf of Cisco Systems (Cisco) in response to the request for comment on a Proposed Rule from the Department of Commerce's Bureau of Industry and Security (BIS) dated May 20, 2015. The Proposed Rule seeks "to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013" It would have the effect of regulating a wide array of technologies used in security research as controlled exports, in the same manner as if they were munitions.¹ We have identified a number of significant concerns that we believe require BIS to revisit the text of the Proposed Rule.²

¹Specifically, the rule would cover: "systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor."

<https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>

² The two issues discussed below (export controls on unpublished vulnerabilities and the demand for source code) are intended to illustrate the nature and depth of our concerns. Cisco has additional concerns and may seek to supplement the record based on whether and how BIS moves forward with the Proposed Rule.



Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

BIS' focus on limiting the cross-border trafficking of weaponized software is well-intentioned, but the current text would cause significant unintended consequences that must be addressed in a revised draft of the Proposed Rule. If implemented in its current form, the Proposed Rule would present significant challenges for security firms that leverage cross border teams, vulnerability research, information sharing, and penetration testing tools to secure global networks, including Cisco. The result would be to negatively impact—rather than to improve—the state of cybersecurity.

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. In order to develop, deliver, manage, and maintain the innovative products and services that Cisco's customers count on to run their businesses, we must engage in complex security research. This requires Cisco to develop and deploy security systems that include intrusion detection, intrusion prevention, next generation firewall, endpoint monitoring, dynamic file capture and analysis, application identification and control, identity management and analysis, and deep content inspection and analysis systems that operate across the extended network and devices.

We need the ability to attack, assess, and strengthen our own technology using sophisticated penetration testing tools. We also rely upon information about unpublished vulnerabilities that we find or that are brought to our attention by outside researchers. In the course of these efforts, we welcome and readily coordinate with expertise from around the globe—and work around the clock.

This level of commitment is necessitated by a dynamic threat environment populated by dedicated, well-resourced adversaries seeking to compromise and undermine the effectiveness of our security investments. These same adversaries can and do readily engage in subversive behaviors. If they discover vulnerabilities before Cisco does, attackers will seek to compromise networks with the intent of controlling systems and manipulating people for their own gain. Many of the activities required to respond to these threats would be restricted or subject to onerous export licensing requirements if the Proposed Rule were adopted.

We understand the importance of the government's concerns regarding the unregulated export of weaponized software. However, many of the same techniques used by attackers are important to developers testing their defenses and developing new effective responses. Cisco needs access to the very tools and techniques that attackers use if we have any hope of maintaining the security of our products and services throughout their anticipated lifecycles. The development of new export control requirements must, therefore, be done carefully and based upon the needs of legitimate security researchers. Otherwise, we will



Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

leave network operators blind to the attacks that may be circulating in the criminal underground—and ultimately blind to the very weaponized software that the proposed rule intends to constrain.

It is our hope that based upon the comments received to the Proposed Rule, BIS will reconsider the text and offer a revised draft. As it does so, there must be a recognition that the success of the IT industry depends upon a global development model. It is unrealistic to expect that all of the resources necessary to secure complex networks will sit inside one country. Implementation of the current text would unnecessarily restrict the sharing of research between teams that work globally in response to discovered threats and vulnerabilities.

Cisco believes the Proposed Rule could stunt the development of valuable avenues of security research—even as attackers continue to innovate freely. BIS has responded to such concerns by pointing out that researchers seeking to export information about unpublished vulnerabilities could take advantage of an exception in the Export Administration Rules (EAR) for information that is already public. According to an FAQ published by BIS: “[u]nder Section 734.7 of the EAR, information that is published, or released at an open conference, is not subject to the EAR.”

The publication of previously unpublished vulnerabilities is not a substitute for reasonable export license exceptions—and could actually cause significant harm to Cisco’s security efforts. Absent adequate license exceptions enabling the security community to quickly share and respond to vulnerability information, the current text would create perverse incentives to publish information about vulnerabilities before developers can mitigate or patch the affected technology. The Proposed Rule could, therefore, unintentionally incentivize the routine publication of previously unknown vulnerabilities without coordination, which would ultimately lead to more zero day exploits.

The security community shares vulnerability information to develop and disclose fixes in a coordinated way. The Department of Commerce’s own National Telecommunications and Infrastructure Administration (NTIA) recently stated that such coordination is so important that it is launching a multistakeholder process entitled “Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure” this September.³ BIS needs to rework its proposal to support NTIA’s efforts. At a minimum, any future iteration of the Proposed Rule should include clear definitions of the controlled items and provide explicit

³<http://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure>



Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

license exceptions enabling legitimate security researchers to share and respond to vulnerability information in a timely manner.

We are also concerned that the proposal calls for the disclosure of source code to the U.S. government. Supplement No. 2 to Part 748—Unique Application and Submission Requirements would require applicants: “[u]pon request, [to] include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.” As the U.S. Government is well aware, developers of information technologies are increasingly facing demands by other governments for disclosure of our intellectual property. Any proposal from the U.S. Government regarding source code disclosure production requirements is extremely damaging.

The concerns listed above are examples demonstrating that the scope of the requirements in the Proposed Rule are far broader than necessary to address BIS’ stated intent—controlling the export of weaponized software. We look forward to working with the Department of Commerce to ensure that the goals of the proposal can be met in a manner that is technology neutral, narrowly tailored to the actual risks faced by the nation, and reflective of the needs of legitimate security researchers seeking to protect the information technologies upon which we increasingly rely. We look forward to continuing the conversation.

Best wishes,

A handwritten signature in blue ink that reads "Eric Wenger".

Eric Wenger, Director Global Government Affairs
Cybersecurity and Privacy Policy
Cisco Systems

PUBLIC SUBMISSION

As of: 7/29/15 3:37 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-hrqq
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0234

Jacob Torrey

Submitter Information

General Comment

See attached

Attachments

Jacob Torrey

Sharron Cook

From: discipleofranok@gmail.com on behalf of Jacob Torrey <jacob@jacobtorrey.com>
Sent: Monday, July 20, 2015 11:14 AM
To: PublicComments
Subject: RIN 0694-AG49 Comment

To Whom it May Concern,

I'm a cyber-security research engineer and I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

Another aspect I'm concerned about will be the reduction in trust placed in US software industries overseas. After the Snowden leaks, there was reduced trust in the safety and security of American-made software. By hampering the bug bounty and exploitation research fields to country-based units, software will be less secure for the consumer, and businesses may shift their purchasing to software not restricted in this way.

V/r,
Jacob Torrey

PUBLIC SUBMISSION

As of: 7/29/15 3:39 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-4hyb
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0235

Jeff Jarmoc

Submitter Information

General Comment

See attached

Attachments

Jeff Jarmoc

Sharron Cook

From: Jeff Jarmoc <jeff@jarmoc.com>
Sent: Monday, July 20, 2015 11:26 AM
To: PublicComments
Subject: Comments on proposed U.S. Wassenaar Arrangement rules

I'm employed as a professional Software Security Consultant, Penetration Tester, and Security Researcher. In this role, I'm tasked by my clients, many of whom are large publicly traded and Fortune 500 organizations, with attempting to subvert the security of their electronic systems, identifying and triaging flaws which can then be remediated. My work has directly helped improve the security of countless organizations. I'm writing to share my comments on the proposed U.S. Wassenaar Arrangement rules.

I'm greatly concerned by the unforeseen impact these new regulations will have on the security industry, and thus the safety and security of US industry in general. I worry that the proposed restrictions may hinder the efforts of US researchers in the free exchange of information and research, and harm the US economy over all.

Please, carefully consider these concerns in reviewing the proposed regulations.

Thank you,
-- Jeff Jarmoc

PUBLIC SUBMISSION

As of: 7/29/15 3:48 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-weel
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0237

Howard Grodin

Submitter Information

General Comment

See attached

Attachments

Howard Grodin

Sharron Cook

From: Howard Grodin <hgrodin@gmail.com>
Sent: Monday, July 20, 2015 12:06 PM
To: PublicComments
Subject: RIN 0694-AG49

Dear Sir or Madam,

I offer the below comments, solicited as part of your review process, out of genuine concern for both the vendors of Penetration Testing tools as well as the legitimate end-users, both corporate and individual.

I strongly believe that the proposal as written is much too broadly worded and puts the legitimate use of, purchase and sale of Penetration Testing tools at risk of harming its legitimate uses in protecting business and consumers from vulnerability exploitations.

Sincerely,

Howard Grodin

Information Security Professional

RE: RIN 0694-AG49 <<https://www.federalregister.gov/r/0694-AG49>>

PUBLIC SUBMISSION

As of: 7/29/15 3:53 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-z5ub
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0238

John Lampe tenable

Submitter Information

General Comment

See attached

Attachments

John Lampe tenable

Sharron Cook

From: John Lampe <jlampe@tenable.com>
Sent: Monday, July 20, 2015 11:25 AM
To: PublicComments
Subject: 0694-AG49

Hello there,

I have worked in Information Security for close to 20 years. I am very concerned with a hasty rush for new Cyber controls without fully understanding the impact to the companies and individuals who work in this space.

Thank You,

John Lampe

PUBLIC SUBMISSION

As of: 7/29/15 3:54 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-bx8b
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0239

Mario Santana risk analytics

Submitter Information

General Comment

See attached

Attachments

Mario Santana risk analytics

PUBLIC SUBMISSION

As of: 7/29/15 3:56 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-ekho
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0240

Keith Seymour

Submitter Information

General Comment

See attached

Attachments

Keith Seymour

PUBLIC SUBMISSION

As of: 7/29/15 3:58 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-47g3
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0241

Kristian erik Hermansen

Submitter Information

General Comment

See attached

Attachments

Kristian erik Hermansen

Sharron Cook

From: Kristian Erik Hermansen <kristian.hermansen@gmail.com>
Sent: Monday, July 20, 2015 1:09 PM
To: kristian.hermansen+bis.doc.gov@gmail.com
Cc: Dave Aitel
Subject: No Cyber Regulations for Penetration Testers

I'm a penetration tester and I'm worried about the unforeseen impact these new Cyber regulations will have on the community, the security industry, and industry at large.

Dave Aitel, CEO of Immunity -- a penetration testing and security services company -- approves this message...

--

Regards,

Kristian Erik Hermansen
<https://www.linkedin.com/in/kristianhermansen>

PUBLIC SUBMISSION

As of: 7/29/15 3:59 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-911g
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0242

Willis Vandevanter

Submitter Information

General Comment

See attached

Attachments

Willis Vandevanter

Sharron Cook

From: Willis Vandevanter <will@silentrobots.com>
Sent: Monday, July 20, 2015 1:12 PM
To: PublicComments
Subject: BIS Cyber Regulations Comments (BIS-2015-0011:RIN 0694-AG49)

Hi!

As a penetration tester and small business owner I am disappointed and concerned with the proposed cyber regulations. The unforeseen impact of these regulations could have far reaching and detrimental effects to the security community and economy as a whole. I empathize with the need to fortify the law and defend against malicious parties. However, the proposed regulations are not the right way.

-Will

In reference to:
BIS-2015-0011
RIN 0694-AG49

PUBLIC SUBMISSION

As of: 7/29/15 5:07 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-upbz
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0243

Matt Weeks

Submitter Information

General Comment

See attached

Attachments

Matt Weeks

Sharron Cook

From: Matt Weeks <matt.weeks@root9b.com>
Sent: Monday, July 20, 2015 1:16 PM
To: PublicComments
Subject: BIS-2015-0011 Comments
Signed By: matt.weeks@root9b.com

Hello,

BIS has requested comments on the proposed Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items. (BIS-2015-0011)

I am the director of the research and development branch of root9B, a US cyber security company. Prior to this, I was an officer in the US Air Force, where I led the Air Force Computer Emergency Response Team (AFCERT)'s Intrusion Forensics unit and Defensive Counter Cyber forces. It was our job to prevent, detect, and respond to cyber security breaches, and I now lead the research and development of software to do the same. In the past, as an individual, I have found and sold zero-day exploit information to defensive security companies who created products to stop those attacks.

Our goal is to increase security, but unfortunately, the proposed rules are too broad and will have negative effects on our legitimate vulnerability and intrusion software research, limiting our ability to defend against cyber intrusions. For example:

1. While I cannot list specific deals due to competitive information, security companies including root9B depend on a robust economy of vulnerability research and threat intelligence. Numerous small businesses focus on finding vulnerability research, exploitation techniques, and intrusion software techniques, and selling the results of their research to security firms like ours and anti-virus companies, as well as many in-house security teams at large corporations, who can act on it to secure their customers and employees. This information all falls under the larger umbrella of threat intelligence, which security companies like root9B both purchase and sell. Such dedicated research firms and full-service security companies are located all over the world.

a. A "policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities" <http://www.federalregister.gov/a/2015-11642/p-22> would be devastating to this industry. We would lose this ability to defend against such attacks since no researcher or small research team could find such attacks and legitimately sell them to security companies. This means that the only outlet for such information would be illegal or government-controlled.

b. Even if the policy of presumptive denial was overturned, many individuals such as myself or companies, like Exodus Intelligence, are recognized world leaders in such research, yet are very small businesses, with fewer than 10 employees, and sometimes only one or two. As research firms, they are identifying new vulnerabilities and exploitation techniques every month. These solidly fall under the description of items to require an export license. To obtain a license for each of these items will consume at least as much effort as developing the items themselves. This is a very different situation than selling physical items or even traditional software, in which you can obtain an export license once, and continue to sell. Because of the nature of vulnerability research, it must be completely new every time.

c. This also poses a significant entry barrier for independent technical researchers working on spare time, as I once was when I was a student at a university; if a license was required, I would not have had any budget or time for the legal application process. I would not have found or sold my zero-day exploits, and millions of users who ran software that was affected would not have been defended. The entry barrier is a large issue, since many researchers have similarly few resources.

d. As a result, research-focused companies will only be able to produce and obtain a license for about half their current output, if at all, either dramatically limiting their productivity or forcing them out of business altogether. Without access to this information, our ability to build defenses to these threats and stay ahead of attackers will be significantly reduced.

2. The proposed regulations (<http://www.federalregister.gov/a/2015-11642/p-21>) also include the statement “that upon request from BIS, the applicant must include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality.” This poses a devastating risk for two reasons:

a. A large portion of the income of many of these research and security firms comes from sales to government security agencies, such as NSA. Compelling us to turn over our source; which is our primary product, for free, is absolutely unacceptable and will prevent us from continuing to do much business.

b. Transferring such information to the BIS will invariably expose this information to foreign intelligence services (FIS's) and cyber criminals, unless BIS is willing to handle all such information with the same protections as highly classified information. Since FIS's and other hostile actors place a high value on vulnerability information, research organizations operate under very similar data security measures. Like almost all organizations, we don't believe BIS or the majority of the US government has the expensive facilities, operation security processes, culture, and equipment necessary to protect this information against advanced cyber adversaries, and we have the experience responding to such breaches to prove it. This is an unnecessary exposure of critically confidential information.

3. The categories of regulated software are also much too broad, and based on a mistaken assumption that there is a clear difference between “intrusion software” and normal software.

a. In reality, to better avoid detection, intrusion software makes every effort to blend in with normal traffic. Communication with malware to steal information goes across the same protocols and uses the same networking tools as normal web, email, file-sharing, and management software. Much of this does not require or use encryption (I dispute that “...most of the items impacted by this rule have encryption capabilities, BIS believes they are already being controlled under Category 5 part 2 of the EAR.” <http://www.federalregister.gov/a/2015-11642/p-36>) Intruders use many programs to obtain information, remotely control systems, which are the same as I have to investigate systems and administrators use to manage systems. The wording throughout this proposal could apply to the majority of network-communicating software and network management software sold by US companies. As a result, it has the potential to expose most US software companies to arbitrary prosecution and/or extensive go-to-market delays and competitive impact obtaining licenses.

b. Security software to monitor system activity for malicious attacks works the same way as “rootkit” software that monitors system activity to steal information. I developed the Ambush Host Intrusion Prevention System (Ambush HIPS), which like all HIPS software uses the same kind of hooks and other techniques as rootkits to monitor system activity. Malicious use could be obtained as just a matter of configuration, as with most software.

c. All bug-finding software falls under the definition of software specially designed for the discovery of zero-day vulnerabilities, yet this class of software is essential for the entire technology industry to find and fix software flaws.

4. I cannot currently answer the questions about how many applications we will need to file of various kinds. I request BIS propose another draft and comment period of at least 3 months to obtain this information.

--

Matthew Weeks

Director, Emerging Technologies root9B

Direct: 262-672-0834

E-mail: matt.weeks@root9b.com

San Antonio Office:

3463 Magic Drive, Suite 225

San Antonio, Texas 78229

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity named. If you are not the named addressee you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Please notify the sender immediately by email if you received this email in error and delete this email from your system. Any views or opinions presented in this e-mail are solely those of the author and do not necessarily represent those of root9B, LLC.

PUBLIC SUBMISSION

As of: 7/29/15 5:21 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-1mjl
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0244

Mike Clark

Submitter Information

General Comment

See attached

Attachments

Mike Clark

Sharron Cook

From: Mike Clark <undefinedspace@gmail.com>
Sent: Monday, July 20, 2015 1:38 PM
To: PublicComments
Subject: RIN 0695-AG49
Attachments: signature.asc

I am a security professional and am worried about unforeseen implications that these new cyber regulations will have on the community, the security industry and national security. Cyber security is a very difficult problem and if researchers cannot share information freely, that could have a significant negative impact. I urge BIS to consider the concerns of industry professionals before implementing any proposed regulations.

Mike

PUBLIC SUBMISSION

As of: 7/29/15 5:22 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-mzvy
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0245

Carbon Dynamics Dan Tentler

Submitter Information

General Comment

See attached

Attachments

Carbon Dynamics Dan Tentler

Sharron Cook

From: Dan Tentler <dan@atenlabs.com>
Sent: Monday, July 20, 2015 3:30 PM
To: PublicComments
Subject: RIN 0694-AG49 Comments

Hello,

I'm the co-founder of a company that conducts tailored security assessments for clients. These regulations would prevent me from being able to travel freely, as I have many devices loaded with tools that would fall under WA and cause a substantial amount of grief.

A secondary effect of security software falling under WA would cause my business untenable amounts of undue grief, extra processes and heartache simply to cope with the regulatory compliance, travel and data transmission aspects of the new laws.

Our goal is to help make the internet safer, by finding problems with businesses that real bad guys would exploit and seeing them fixed in front of our own eyes. Our goal is to prevent things like the Home Depot, Target, Anthem and OPM breaches. We have seen fist-hand the improvement of our clients, solely based on our efforts.

This proposed legislature makes it harder for us to do that.

And the real bad guys certainly won't be following these rules.

This effectively disarms the good guys. Only law abiding citizens will obey these proposed regulations.

Please don't stop us from making the internet safer!

-Dan Tentler
Co-Founder, Carbon Dynamics

PUBLIC SUBMISSION

As of: 7/29/15 5:23 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-fobq
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0246

Sandra Bittner

Submitter Information

General Comment

See attached

Attachments

Sandra Bittner

Sharron Cook

From: Sandra.Bittner@aps.com
Sent: Monday, July 20, 2015 3:53 PM
To: PublicComments
Cc: Sandra.Bittner@aps.com
Subject: RIN 0694-AG49 BIS-2015-0011

I suggest this regulation be denied and moved to sub-committee for further consideration and review.

The provisions as specified “systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology” essentially penetration testing frameworks, software, digital forensic toolkits, network vulnerability and intrusion, tools, techniques and methods, anomaly detection and monitoring, I assert would damage research and researchers, increase complexity and costs for defenders while further limiting an already small toolset while having no positive impact on the criminal elements the treaty likely was targeting.

Additionally, the agreement stands in opposition to what IS required, in order to, adequately address the current problem. Specifically, more open unrestricted international sharing of security research, computer science, information science, analytic science, open science, networking, grid-technologies, distributed computing, grid computing, cloud computing, whether labeled information security, cyber security, computer science, networking science, vulnerability information and tools, methods and techniques, etc, required to win against highly capable criminals. Further this regulation would hamper the development of the cyber/information security firms, tools, methods, techniques and restrict their competitive nature giving other countries an edge over the USA. Allowing them to prosper at the expense of the USA. This agreement hampers the prosperous development of next generation products, services, firms, and talent necessary to not only compete at an international level but to dominate it through talent, economics and sharing. At a practical level, it will reduce the effectiveness and availability of software, tools, methods, techniques , protocols or frameworks, required to defend critical infrastructure within the USA and international US-based companies. Further smaller communities with highly restricted budgets such as public municipalities and individual owner/operators in small communities will be hurt as they tune and tweak these tools (currently paid for by other communities) and released in community versions for their use. These communities are some of the largest adopters of community codes, tools, test kits, detection software, etc. They do not have suitable budgets or the talents necessary to accommodate the magnitude of products and development efforts that would be negatively impacted by enactment of this regulation.

I encourage those considering the implementation of the treaty (a treaty which truly needs more work) to use the opportunity to support the continued prosperous open development and open distribution of these crucial software tools, methods, techniques, protocols or frameworks to all communities without restriction. It is recognized that the criminal element has found alternative non-standard uses for some of the tools and likely always will. The key is to not disturb the work in progress of the remaining legitimate communities that create, use, adapt, create derived works of,

develop, implement, research, experiment with, or build on existing software, tools, methods, techniques , protocols or frameworks.

In my experience sometimes the complexity of digital gets in the way of understanding. Consider therefore a practical common boring tool from construction, a hammer. A hammer is a key tool to building and creating new things such as houses, fine furniture, etc. It is true someone could abuse it for a non-normal use however regulating the manufacture, production, design and development, operation, or delivery of, or communication with such a tool is absurd . This regulation and the treaty itself appears to attempt to regulate the generation, operation or delivery of, communication with, development or production of digital hammers and should therefore be considered equally absurd.

Do not penalize the practitioners (defenders) because savvy criminals have discovered malicious non-normal uses for legitimate tools. In so doing, the regulation will only confuse things further. It may also cause some of the best defenders and researchers to give up on the problem because it continues to get more difficult to help do the right thing – due to “well-intentioned” but useless, burdensome restrictions.

In conclusion, the BIS proposal for instituting a “license for the export, re-export, or transfer (in-country) of these cybersecurity items to all destinations, except Canada.” should be denied. The proposal to review new policies and special submission requirements for cyber security controls and to add the definition of “intrusion software” into the definitions section should also be denied. Find a less intrusive way to implement that supports the open sharing of information, software, tools, methods, techniques , protocols and frameworks without restriction or cancel the US participation in the treaty.

Respectfully,

Sandra Bittner

SANDRA BITTNER, CISSP

Arizona Public Service

Palo Verde Nuclear Generating Station

Cyber Security Project

5801 S. Wintersburg Road, M.S. 7098

Tonopah, Arizona 85354

Tel 623-393-4218

PUBLIC SUBMISSION

As of: 7/29/15 5:26 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-kzn1
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0247

API cover memo Aaron P Padilla

Submitter Information

General Comment

See attached

Attachments

API cover memo Aaron P Padilla



AMERICAN PETROLEUM INSTITUTE

Aaron P. Padilla

Senior Advisor, International Policy

1220 L Street, NW
Washington, DC 20005-4070
Telephone (202) 682-8468
Fax (202) 682-8408
Email padillaa@api.org
www.api.org

July 20, 2015

Catherine Wheeler
Director, Information Technology Control Division
Regulatory Policy Division
Bureau of Industry and Security (BIS)
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

Subject: **RIN 0694-AG49** – Notice of Request for Public Comment Regarding Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Ms. Wheeler:

The American Petroleum Institute (API) welcomes the opportunity to comment upon the US Department of Commerce Bureau of Industry and Security (BIS) Notice of Request for Public Comment Regarding Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items.

API is a national trade association that represents all segments of America's oil and natural gas industry. Its more than 600 members include large integrated companies, exploration and production, refining, marketing, pipeline, and marine businesses, and service and supply firms.

Cybersecurity is a public policy priority for API. The proposed BIS rule on intrusion and surveillance items would significantly restrict API's multinational member companies' cyber defense efforts by triggering a significant administrative burden of export license applications and restricting routine testing and research into potential cyber vulnerabilities and exploits ("intra-company transfers or internal use"). ***API member companies strongly urge BIS to reconsider and rewrite the proposed rule in order to address the concerns articulated below in responses to each of the questions in the Request for Public Comment.***

- 1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:**
 - a. How many additional applications would be for products that are currently eligible for license exceptions?**
 - b. How many additional applications would be for products that currently are classified EAR99?**

Under the narrowest interpretation of the proposed rule, each individual API member company that operates outside the United States or Canada would need to submit hundreds and potentially thousands of additional license applications.

Under the broadest interpretation of the proposed rule, each individual API member company that operates outside the United States or Canada may need to submit tens of thousands to hundreds of thousands of additional license applications; this is because the rule could be interpreted broadly to apply to any “systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software” – with “communication with intrusion software” standing alone (because of the immediate preceding “or”) rather than being coupled with “generation, operation or delivery of...intrusion software.” This interpretation would implicate intra-company data transfers, workstation installations, Windows instances, software languages/shells and management platforms (such as SAP) of company employees located or traveling overseas – since these examples are all tools used for companies’ internal application development and are also required for the communication with intrusion software.

While the expanded [BIS FAQs on the proposed rule](#) seem to indicate a narrower interpretation of the proposed rule, and would therefore grant more export license exemptions to US companies, the language of the proposed rule itself is not as precise.

API recommends that BIS re-write the proposed rule and offer narrower definitions to exclude as much as possible from export controls any broad interpretation that would implicate the following: intra-company data transfers, workstation installations, Windows instances, software languages/shells and management platforms (such as SAP) of company employees located or traveling overseas and the use of such tools for software development with legitimate purposes or for cyber defense (see #3 below).

- 2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?**

Under the narrowest interpretation of the proposed rule, each individual API member company that operates outside the United States or Canada would need to submit hundreds and potentially thousands of additional deemed export, reexport or transfer (in-country) license applications.

Under the broadest interpretation of the proposed rule, each individual API member company that operates outside the United States or Canada would need to submit millions of additional deemed export, reexport or transfer (in-country) license applications. This broad interpretation of the rule would require license applications for each instance of any non-US or non-Canadian citizen within the firm accessing software that underpins the development of intrusion software *or* communication with intrusion software. If BIS were to enact the proposed

rule, according to this broad interpretation, it may also have the undesirable effect of encouraging software development overseas rather than within the US in order for companies to avoid the burden of licenses.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how?

Yes, the proposed rule would significantly restrict API's multinational member companies in their cyber defense efforts. The proposed rule would restrict internal cybersecurity "red teams" as they test the companies' potential cyber vulnerabilities by trying to identify and exploit the companies' networks. The proposed rule would also restrict testing and research into cyber vulnerabilities ("intra-company transfers or internal use").

It is problematic that the proposed rule would require export licenses for the use of penetration tools that scan for vulnerabilities and extract some data for "proof of concept" of successfully identifying any vulnerability. In addition, the proposed rule's exclusion of open source/public tools (like Metasploit) does not offer sufficient export license exemption because it is common for API member companies to use proprietary penetration testing software (either developed in-house or from a vendor). Use of such proprietary penetration tools is a common and effective part of API member companies' cyber defense programs, and it would be onerous to have to apply for export licenses for such activities.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

Each individual API member company that operates outside the United States or Canada, per application, would need to spend tens of hours. Under the narrowest interpretation of the proposed rule, the number of applications per company would be hundreds and potentially thousands; resulting in additional effort of hundreds to thousands of days of additional time to answer the questions. Under the broadest interpretation of the proposed rule, the number of applications per company would be tens of thousands to hundreds of thousands, resulting in additional effort of thousands of days of additional time to answer the questions.

The most pertinent sections of the proposed rule that would require this effort by API member companies are the following requirements for information:

- (i) Whether the cybersecurity item has encryption or other "information security" functionality, Encryption Registration Number (ERN) and encryption Commodity Classification Application Tracking System (CCATS) number(s);
- (ii) Whether the cybersecurity item has been previously classified or included in a license application submitted on or after May 20, 2015 for which all requirements of this section (including the questions set forth in paragraph (z)(1)(iii) of this section) have been satisfied. If so, then provide the Commodity Classification Automated Tracking System (CCATS) number(s) or issued license number(s).
- (iii) If the cybersecurity item has not been previously classified or included in a license application, then:
 - (A) Describe the cybersecurity functions and user interfaces (e.g., Application Programming Interfaces (APIs), Command Line Interfaces (CLIs) or Graphical User Interfaces (GUIs)) that are implemented and/or supported. Explain which are for internal use private to the developer of the product, and/or which are for use by the customer or other operator.

Department of Commerce, Bureau of Industry Security (BIS)

July 20, 2015

Page 4

(B) Describe the cybersecurity functionality (including as related to “intrusion software”) that is provided by third-party frameworks, platforms, tools, modules or components (if any). Identify the manufacturers of the cybersecurity items, including specific part numbers and version information as needed to describe the item. As applicable, describe whether the third-party cybersecurity software is statically or dynamically linked.

(C) For items related to “intrusion software,” describe how rootkit or zero-day exploit functionality is precluded from the item. Otherwise, for items that incorporate or otherwise support rootkit or zero-day exploit functionality, this must be explicitly stated in the application.

We appreciate the opportunity to comment on the proposed rule, and we would welcome the opportunity to work collaboratively with BIS staff going forward to address the concerns outlined in this response. Should you have any questions or would like to discuss further, please feel free to contact me at (202) 682-8468 or PadillaA@api.org.

Sincerely,

A handwritten signature in cursive script that reads "Aaron Padilla".

Aaron Padilla
Senior Advisor, International Policy
API

PUBLIC SUBMISSION

As of: 7/29/15 5:29 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-7kjn
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0248

Thomas Dulien

Submitter Information

General Comment

See attached

Attachments

Thomas Dulien

Sharron Cook

From: Thomas Dullien <thomas.dullien@googlemail.com>
Sent: Monday, July 20, 2015 6:59 PM
To: PublicComments
Subject: BIS-2015-0011 Comments

Dear Sirs,

I am a renowned information security expert with a long history of developing novel techniques and technologies which help understand attacks and attacker capabilities better. Algorithms for the comparison of binary code that I developed won Germany's biggest privately financed research award in the natural sciences and have entered standard operation in many Antivirus companies. Recently, I was heavily involved with researching a hardware issue called "Rowhammer", which had significant industry-wide impact. I am currently employed at Google.

The proposed rules, as they stand today, are extremely harmful to security research and any efforts at defending IT systems. This is partially due to a dangerously overbroad definition of "intrusion software" in the original Wassenaar amendments - but also due to specific extensions introduced by the proposed implementation.

The biggest problems with the current rules are unclear and hard-to-interpret definitions of what exactly is controlled. Even after several telephone conferences with the BIS, and months of discussion, it is unclear to lawyers with a background both in technology and export regulations what technologies and software would actually fall under the new regulations.

The second large problem is the disastrous effect this legal uncertainty will have on security research. Most security research that helps improve Internet security is performed by companies and entities that have no experience with (nor desire to acquire such experience) export controls. The proposed rules would worsen the cost/benefit calculation in many organisations, and simply lead to much less research that improves security being performed. Security research with the purpose of defense is a cost center in most organisations. At the same time, offensive security research that remains non-public (and thus makes everybody more vulnerable to surveillance and data theft) would continue unhindered - for attackers that keep things secret, this research is a profit center, and they can just shift additional compliance cost to their customers.

There are many more problems in the details of this proposal, but I hope they will be addressed by other comments.

Concrete policy recommendations from my side are:

1) When defining "intrusion software", much narrower phrasing should be adopted to ensure that security research can proceed unencumbered. The focus should be on systems that combine the following features:

- ** Identification of individuals in very large datastreams or groups with intent of
- ** injecting or modifying network traffic with intent of
- ** illicitly accessing data of that individual

By combining these requirements, injection proxies that infect executable downloads would be covered in the same way as logic issues in browsers that leak sensitive information - the overly

specific and faux-technical phrasing of Wassenaar would be replaced with something that causes less collateral damage to security research while covering the technologies that were the targets of the Wassenaar amendments comprehensively.

By focusing on illicit access, legitimate penetration testing tools that would be used with the knowledge and consent of the owner of the targeted computers would also be exempted from export control.

2) The comment period on the proposed regulations should be extended, and more people with explicit background in security research should be consulted early in the process of drafting alternative, less harmful and more effective proposals. This may require convening a group of researchers and have them work for a few days in the same room as the people drafting the proposal for regulation.

3) Explicit exemptions for transmitting information without payment, and intra-company-transfers, and for transmitting information with defensive intent/purpose need to be carved out to ensure that any work that will ultimately benefit IT security will be easily identified as "not covered by export controls".

In general, I agree with the statement of my current employer - the current wording of Wassenaar should be changed, because it is this overly broad wording that causes a lot of the problems downstream.

Computer security is very different from "traditional" export control. Vulnerabilities bear very little resemblance to "real" controlled goods - because I can render an exploit useless to hundreds of attackers by just providing it to the vendor to fix it. The export of "traditional" controlled goods rarely serves the purpose of making the entire world less vulnerable to attack - but the free flow of information about computer attacks is an absolute necessity if we wish to build a safer and more reliable internet.

Cheers,
Thomas Dullien

PUBLIC SUBMISSION

As of: 7/29/15 5:31 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-kq80
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0249

Alan Saqui

Submitter Information

General Comment

See attached

Attachments

Alan Saqui

Sharron Cook

From: Alan Saqui <alan.saqui@gmail.com>
Sent: Monday, July 20, 2015 8:53 PM
To: PublicComments
Subject: Comment for RIN 0694-AG49

To Whom It May Concern:

My name is Alan Saqui, and I am a security assessment engineer at Arbor Networks responsible for overseeing the internal security of our products. I am deeply worried about the unforeseen impact these new Cyber regulations will have not only my ability to do my job, but also on the community, the security industry, and industry at large.

Thanks,
Alan

PUBLIC SUBMISSION

As of: 7/29/15 5:33 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-9sz3
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0250

Rochester Institute of Technology Peter Ryan Jr

Submitter Information

General Comment

See attached

Attachments

Rochester Institute of Technology Peter Ryan Jr

Sharron Cook

From: Peter Ryan, Jr. <phr8276@rit.edu>
Sent: Monday, July 20, 2015 10:02 PM
To: PublicComments
Subject: Wassenaar

As a young cyber security professional and current student these proposed rules are even troubling to me. The time, energy, and hard work put into the field by researchers does a great deal to contribute to the overall safety of the Internet and connected network devices. America enjoys an offensive advantage in the cyber domain and this position is supported by the work that the proposed rules could prohibit. Security work, especially in support of our national interests, will suffer and other nations, often our foes, will capitalize on their freedom to undertake this work, hurting US industry for the long term.

--

Peter Ryan, Jr. '15
BS, Computing Security
Public Relations Chairman and Webmaster, Sigma Chi - Lambda Kappa
Social Media Ambassador Captain, Office of Admissions
Rochester Institute of Technology

PUBLIC SUBMISSION

As of: 7/29/15 5:37 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-cms5
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0251

Chris Sullo

Submitter Information

General Comment

See attached

Attachments

Chris Sullo

Sharron Cook

From: Sullo <csullo@gmail.com>
Sent: Monday, July 20, 2015 11:59 PM
To: PublicComments
Subject: BIS-2015-0011

As a professional penetration tester and open source software author, I think BIS-2015-0011 would be a huge detriment to the security industry and thus the security of US companies. The vague wording and unknown repercussions make BIS-2015-0011 one of the most dangerous pieces of legislation to be seen in recent memory. Please do not adopt BIS-2015-0011!

Thank you,
Chris Sullo
Chesterfield, VA

PUBLIC SUBMISSION

As of: 7/29/15 5:44 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-rmnf
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0253

Michael Hunter

Submitter Information

General Comment

See attached

Attachments

Michael Hunter

Sharron Cook

From: Michael Hunter <mhunter@lusars.net>
Sent: Tuesday, July 21, 2015 1:57 AM
To: PublicComments
Subject: concern about "intrusion software"

Greetings,

I am a computer security professional working at a Fortune 500 high tech manufacturer. I read a recent Google Security blog about upcoming changes to the Wassenaar agreement:

<http://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html?m=1>

I am concerned that U.S. policy is headed down the wrong path and that we will end up in a similar situation similar to the 90s where cryptography implementations faced undue restrictions in the U.S. I urge that the U.S. government ensure that only scenarios that are clearly dangerous to U.S. interests be illegal and that other uses -- including as described in the Google blog -- be explicitly endorsed.

Thank you,
Mike Hunter

PUBLIC SUBMISSION

As of: 7/29/15 5:46 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-h3um
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0254

West Coile

Submitter Information

General Comment

See attached

Attachments

West Coile

Sharron Cook

From: West Coile <wcoile@gmail.com>
Sent: Tuesday, July 21, 2015 9:43 AM
To: PublicComments
Subject: RIN 0694-AG49

I have worked in cyber security for many years. While I am sure these proposed RIN 0694-AG49 <<https://www.federalregister.gov/r/0694-AG49>> regulations are surely well intentioned, I fear they may have side effects that would in fact harm the security and research communities, and may be detrimental to american interests.

PUBLIC SUBMISSION

As of: 7/29/15 5:49 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-jjns
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0255

David A Wheeler

Submitter Information

General Comment

See attached

Attachments

David A Wheeler

Sharron Cook

From: David A. Wheeler <dwheeler@dwheeler.com>
Sent: Tuesday, July 21, 2015 10:58 AM
To: PublicComments
Subject: Proposed rule RIN 0694-AG49 should be REJECTED

Please REJECT proposed rule RIN 0694-AG49 (“Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items”). This proposal would make “intrusion software” export-controlled, covering “systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices.” Here are some reasons to reject it.

First, this proposed rule will make U.S. computer systems much LESS SECURE. It is standard practice for organizations to attack their own systems before they are deployed, using the very tools being proposed for export control, so they can detect vulnerabilities before attackers do. Export controls will not inhibit attackers, but export controls will inhibit tool use by defenders, leaving US systems more vulnerable to attack.

Second, this proposed rule will REDUCE or ELIMINATE AMERICAN JOBS in an important sector, and make the United States much more dependent on systems controlled by foreign companies. Industry will simply move such operations outside the United States and fire many U.S. employees. This has happened before. The “crypto wars” in the 1990s, which attempted to impose robust export controls on cryptography, did not prevent the use of cryptography. Instead, export controls caused a flight of cryptographic expertise to other countries.

Third, this proposed rule is UNENFORCEABLE. The key essence of “intrusion software” is typically small pieces of code. These are trivially encrypted and sent worldwide.

Fourth, this will INHIBIT U.S. research and development (R&D) in cybersecurity, putting the United States at a technological disadvantage. A key way that researchers and practitioners share techniques is by sharing code that demonstrates a concept. If U.S. citizens cannot publicly publish their work, others will be able to carry on and quickly surpass the United States. Separating “offense” from “defense” is impractical; offensive code is needed to test systems, and authors of defensive systems often need the latest attack information. Software code is the primary language used to share this information.

Fifth, this is LEGALLY SUSPECT; it may be unconstitutional because it inhibits free speech. There is an increased understanding that software code is a form of speech (aka “code is speech”). For example, in *Universal City Studios v. Corley*, {FN191: 273 F.3d 429, 60 USPQ2d 1953 (2nd Cir. 2001)} the Second Circuit said, “Instructions that communicate information comprehensible to a human qualify as speech whether the instructions are designed for execution by a computer or a human (or both). {FN193: 273 F.3d at 447-448, 60 USPQ2d at 1964-1965}” <http://digital-law-online.info/lpdi1.0/treatise50.html>. Similarly, Judge Patel found that, “This court can find no meaningful difference between computer language... and German or French.... computer language is just that, language, and it communicates information either to a computer or to those who can read it....” <https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech>

I am speaking only for myself as a U.S. citizen, and not as a representative of any organization. My credentials include a PhD in Information Technology, a certificate in Information Systems Security, an MS in Computer Science, and a BS in Electronics Engineering, all from George Mason University (GMU) of Fairfax, VA. I also teach a graduate-level course at GMU on how to develop secure software.

Thank you for your time.

--- Dr. David A. Wheeler, PhD. < dwheeler @ dwheeler . com >

PUBLIC SUBMISSION

As of: 7/29/15 5:51 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k96-9a89
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0256

JD Postage

Submitter Information

General Comment

See attached

Attachments

JD Postage

Sharron Cook

From: JD <jdpostage@linuxmail.org>
Sent: Tuesday, July 21, 2015 3:16 PM
To: PublicComments
Subject: Wassenaar Arrangement

Hello,

I recently read this blog post from Google along with a supporting news article and am quite confused about the intended outcome of this new legislation.

<http://googleonlinesecurity.blogspot.com/2015/07/google-wassenaar-arrangement-and.html>

As with export encryption in the 90's, it seems highly implausible to me that you're going to reliably keep new exploits or software for exploits and detecting them out of the hands of countries that go bump in the night. What you *will* plausibly do is hinder and cripple large multinationals to perform adequate security testing and report vulnerabilities. That's a much bigger problem than the one the proposed changes seem intended to solve even if they worked as advertised.

PUBLIC SUBMISSION

As of: 7/29/15 6:11 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-rrej
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0257

ViaSat BIS-2015-0011 Comment 7-29

Submitter Information

General Comment

See attached

Attachments

ViaSat BIS-2015-0011 Comment 7-29



6155 El Camino Real
Carlsbad, CA 92009-1602
Tel: (760) 476-2200
Fax: (760) 929-3941

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, N.W.
Washington, DC 20230
Submitted electronically via e-mail

Attn: Catherine Wheeler, Director, Information Technology Control Division

Re: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Mrs. Wheeler,

ViaSat appreciates the opportunity to provide the following comment to proposed implementation of the Wassenaar Arrangement 2013 Plenary Agreements Implementation of controls on Intrusion and Surveillance Items. The aim of this comment is to address who we are and what we do, outline the impact of the controls as implemented in the proposed rule, and provide possible alternate language for your consideration.

Background

ViaSat is an Internet Service Provider (ISP) to the global consumer market using digital satellite communications, ground network systems, and other wireless networking and signal processing equipment. ViaSat also develops and manufactures satellite antenna systems, data link terminals, information security for networking, mobile IP networking, communications microprocessor chipsets, and communications simulation and training systems. ViaSat is headquartered in Carlsbad, California. Additional information about ViaSat is available at www.viasat.com.

Under the brand name Exede® (www.exede.com), ViaSat has shown that satellite has become another way to provide broadband internet services to the home in a way that matches speed, capacity, and price of terrestrial broadband. In addition to providing broadband satellite internet service to the home, ViaSat employs the Exede® network architecture to provide mobile broadband satellite internet services comparable to in-home service to airline passengers through Exede® In The Air (www.viasat.com/exede-in-the-air).

The current Exede® service is provided by ViaSat-1, the most powerful communications satellite in orbit around the Earth today. The footprint for ViaSat-1 is currently limited to the United States and Canada. ViaSat manages its network within the United States, while the Canadian footprint is managed within Canada by our strategic partner.

In 2016, ViaSat plans to launch the next generation of high capacity Ka-band satellites, ViaSat-2, which will have double the bandwidth economics and seven times the coverage area of ViaSat-1. This coverage area will extend across the Atlantic Ocean and provide limited service over the British Isles and will link up with other Ka-band satellites in Europe, such as KA-SAT which is operated by Eutelsat.

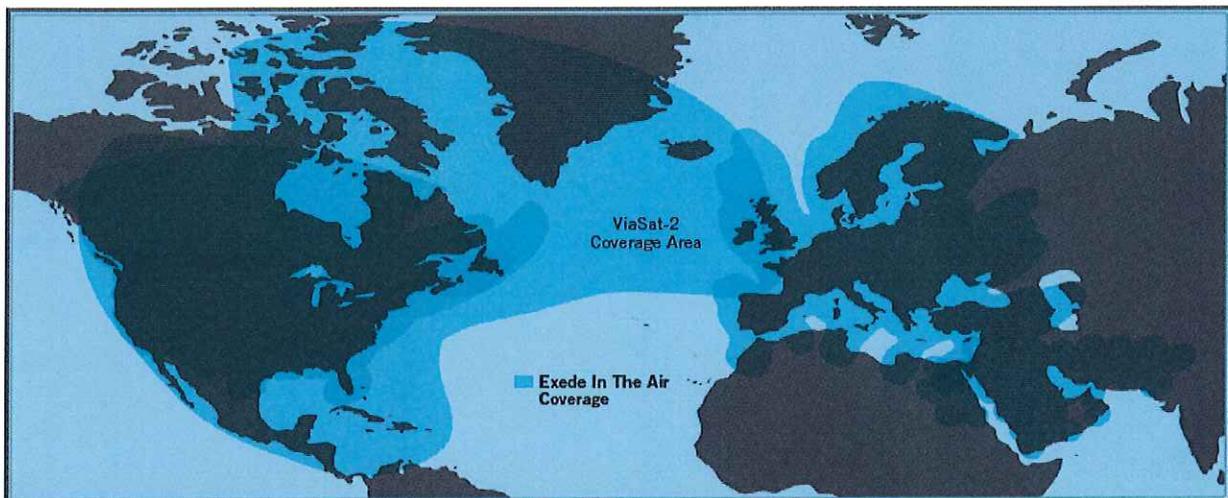


Figure 1 – Planned coverage area for Exede® In The Air

Not only is ViaSat an Internet Service Provider, but we are also a technology supplier to the Ka-band satellite market. ViaSat has developed an exceptional group of technologies to help design, build, and implement Ka-band satellite networks around the world, such as:

- The SurfBeam® user terminal
- The leading Ka-band satellite ODU
- DVB S2 SkyPhy® ASICs
- Network and application acceleration software
- Ka-band satellite antennas and gateway systems
- Satellite payload and system design

These technologies, and others, are currently being utilized or implemented in Europe, the Middle East, and Australia, with expected expansion in the future.

ViaSat believes network protection and security is a necessity in the 21st century, not only for its own network, but also for other service providers utilizing ViaSat provided equipment. As such, ViaSat has developed hardware and software tools and equipment to both test for network vulnerabilities and monitor IP networks for malicious activity, which is the subject of the proposed rule published May 20, 2015.

Impacts

The proposed rule on the Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items seeks to introduce controls on two distinct categories of cybersecurity items: a) intrusion and b) surveillance.

ViaSat seeks to take a holistic approach to cybersecurity within its networks, requiring both thorough testing of network to assess its vulnerabilities and constant auditing of a defended network. The proposed rule has a potential impact on both of these activities. There is obviously not an impact on ViaSat's purely domestic network activities, but there may be an impact when assisting foreign partners on the design and development of their networks utilizing ViaSat equipment or when engaging non-U.S. ViaSat locations in the development of penetration testing or network surveillance tools.

As the proposed rule states, these types of products most likely are currently controlled for some encryption functionality, enabling the use of License Exception ENC in most instances. Specifically, 740.17(a)(1) &(a)(2) would have allowed for the development and production of these items, whereas the new rule would create licensing requirements for this activity involving foreign nationals or foreign sites outside of Canada.

ViaSat has been involved in the design and implementation of satellite internet networks in multiple international destinations that would meet the definition of "carrier class"¹ as defined in BIS' FAQ on Intrusion and Surveillance Items and is currently developing equipment and software that will meet the established control parameters as established in the subparagraphs to 5A001.j. The Wassenaar Arrangement has acknowledged that not all uses of this equipment are for malicious or predatory activities by creating a decontrol note to 5A001.j. ViaSat applauds the allowance of the three excepted activities of marketing purposes, network quality of service (QoS), and network quality of experience (QoE) but notes the lack of exceptions for intrusion.

BIS has asked specific questions be answered as related to this comment and ViaSat will now directly respond to those questions:

1. How many additional license applications would your company be required to submit per year under the requirements of this proposed rule?

ViaSat is still undergoing the analysis to determine the full extent of those items that may require a license under this rule. However, we do anticipate that there are items that do not currently require licensing that would be impacted by this rule, and this number is not insignificant to ViaSat.

Specifically, commodities and technology that previously would have been eligible for license exception ENC would now require licensing.

¹ The term "carrier class IP network" is meant to specify systems that sit at a national level (or large regional) IP backbone and handle data from an entire city or country. In terms of IP network surveillance systems, this is meant to exclude systems that can only handle smaller data streams or networks, such as those for a campus or a neighborhood. This control does not capture systems that can only analyze data from one person or a small group of people at a time.

a. How many additional applications would be for products that are currently eligible for license exceptions?

We believe that any product that would be impacted by this rule would not require licensing as the EAR is currently written and most would likely qualify for license exception ENC.

b. How many additional applications would be for products that currently are classified EAR99?

ViaSat does not believe any of its affected items would be classified under EAR99.

2. How many deemed export, reexport or transfer (in-country) license applications would your company be required to submit per year under the requirements of this rule?

While ViaSat cannot provide an exact number, we believe a significant portion of the licenses required by the changes proposed in this rule would be deemed export licenses.

3. Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.

ViaSat believes this to be the single largest impact of this proposed rule. ViaSat is an international service provider and equipment provider with foreign locations that participate in the development and production of equipment and software that would potentially be affected by this rule. As a result, international networks may be more susceptible than their U.S. counterparts which may create vulnerabilities when interconnecting networks.

4. How long would it take you to answer the questions in proposed paragraph (z) to Supplement No. 2 to part 748? Is this information you already have for your products?

ViaSat believes it would take roughly the same amount of time to answer the questions in paragraph (z) as it currently does to complete Supplement 6 to Part 742 for encryption items. Currently some, but not all, of the information required by paragraph (z) is captured due to other classification requirements elsewhere in the EAR.

Recommendations

As part of our comment letter, ViaSat is submitting possible language additions that would address and eliminate the potential impacts to ViaSat's business this regulatory change would cause while maintaining the intent of the language change. Our recommended solutions are as follows:

Solution #1: Create additional positive or allowed uses:

ViaSat recommends acknowledging the role of the service provider as it relates to security within a network. As the use of the internet becomes ever more entangled with every day activities, the likelihood that malicious actors will attempt to profit increases. ViaSat takes its role as a service provider very seriously and seeks to protect its users and customers from any harm that may come if a network is somehow comprised. One may say that network protection could be included in the definition of QoS or QoE, but ViaSat believes those terms are ill-defined

and this activity stands on its own. The activity of ensuring network protection should be allowed in the exceptions for network surveillance items, as below:

Note: 5A001.j does not apply to “systems” or “equipment”, “specially designed” for any of the following:

...

d. Network security or protection.

Solution #2: Extend surveillance exceptions to intrusion items:

When creating the controls on network surveillance equipment, the Wassenaar member states acknowledged that despite the ability for this equipment to be used in a malicious or predatory manner, there were distinct beneficial, ethical, and commercially acceptable uses of this equipment. The note to 5A001.j does not rely upon a technical basis to separate “offensive” from “defensive” uses of surveillance items, and ViaSat believes the same benefit could be extended to the ECCNs created for intrusion software hardware, software, and/or technology. For instance, ECCN 4A005 could be amended with the following note:

Note: 4A005 does not apply to “systems” or “equipment”, “specially designed” for network security or protection.

Examples of network security or protection include, but are not limited to:

- a. Assessing security vulnerabilities;*
- b. Conducting threat analyses; or*
- c. Determining cybersecurity risks.*

Adding exceptions or notes such as the one above to ECCNs 4A005, 4D001, 4D005, and 4E001 would serve to allow the ‘good guys’ to continue to perform their legitimate security activities, while still capturing the malicious activities of the ‘bad guys’.

Solution #3: Narrow the definition of intrusion software:

Intrusion software, as defined, is a wide definition that may unintentionally capture software that is not malicious in nature. Specific items captured by the definition of intrusion software as currently written, and the hardware, software, and technology associated with those items, are systems that are defensive in nature. ViaSat believes that the definition could be modified in the following manner to remove these items from scope of control:

Notes: 1. “Intrusion software” does not include any of the following:

...

d. “Software” designed to be installed by manufacturers, administrators or users, for the purposes of network security or protection.

Clarification

In addition to the recommended language additions, ViaSat seeks clarification to the license requirements for ECCN 5A001.j. The related controls to this ECCN state that equipment not meeting all of the technical requirements to this ECCN are controlled under other ECCNs, but

that equipment may not be sold separately if it is known that it will be used within a system that is described in 5A001.j. ViaSat has a few questions related to the implementation of this note:

- Is this note a complete prohibition on the sale of equipment related to ECCN 5A001.j or does it create an end-use based licensing requirement? If a strict prohibition, should it be cross-referenced elsewhere in the EAR so that exporters do not miss such an extreme exclusion? If an end-use based licensing requirement, should this licensing requirement be moved to Part 744 to be more consistent with the rest of the EAR?
- The note specifically mentions equipment with some, but not all, of the features contained within 5A001.j. If equipment has none of the features described in the ECCN, but is to be used in a system described in 5A001.j, would that equipment fall under the purview of this note? Does this note apply to any item subject to the EAR?

Conclusion

As requested in the proposed rule, ViaSat has provided information related to the controls introduced on intrusion and surveillance equipment. In addition, ViaSat has outlined the potential impact of this change to our business and provided possible remedies that we believe would address and eliminate that impact.

If you require any further information, please contact me at (760) 893-2918 or via email at joshua.millan@viasat.com.

Sincerely,

ViaSat, Inc.



Joshua Millan
Global Trade Compliance

PUBLIC SUBMISSION

As of: 7/29/15 6:13 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-e9lm
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0258

USTelecom anthon V Jones 7-29

Submitter Information

General Comment

See attached

Attachments

USTelecom anthon V Jones 7-29



July 20, 2015

Via: Electronic Submission (www.regulations.gov)

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave, N.W.
Washington, DC 20230

Attn: Catherine Wheeler, Director, Information Technology Control Division

Ref: RIN 0694-AG49

Subject: Comments Regarding Proposed Rulemaking Implementing Wassenaar Arrangement 2013 Plenary Agreements; Intrusion and Surveillance Items

Dear Ms. Wheeler:

The United States Telecom Association (USTelecom)¹ submits these comments to the Department of Commerce, Bureau of Industry and Security (Department) regarding its proposed implementation of the Wassenaar Arrangement 2013 Plenary Agreements (Wassenaar Agreement) relating to intrusion and surveillance items.² USTelecom is concerned that the Department's proposed rules are too broad and would have the unintended consequence of hindering the telecommunication industry's ability to monitor networks, including their own, for vulnerabilities. Moreover, unless the Department incorporates additional flexibility with respect to the licensing requirements, the proposed rules could significantly hamper cybersecurity activity and information sharing between industry stakeholders and government partners.

¹ USTelecom is the premier trade association representing service providers and suppliers for the telecom industry. Its diverse member base ranges from large publicly traded communications corporations to small companies and cooperatives – all providing advanced communications service to both urban and rural markets. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

² Department of Commerce, Bureau of Industry and Security, Federal Register Notice, *Wassenaar Arrangement 2013 Plenary, Agreements Implementation: Intrusion and Surveillance Items*, 80 FR 28853, May 20, 2015.

USTelecom maintains that, while well-intentioned, the Department's proposed rules will hinder the need for responsiveness and speed in the nation's cybersecurity efforts by constructing unnecessary bureaucratic hurdles that will hinder beneficial cybersecurity activity. Despite the broad government acknowledgement on the need for speed and flexibility within the private sector in the area of cybersecurity, the Department would be inserting a significant barrier to such capabilities with its proposed rules. While acknowledging the Department's need to implement the Wassenaar Agreement, such implementation should not be at the expense of continued development of robust and responsive cybersecurity activities and procedures.

The Role of USTelecom Member Companies in Cybersecurity Activities

Many of USTelecom's member companies are actively engaged in the detection, prevention and mitigation of harms resulting from cybersecurity threats. USTelecom and its member companies have been involved in these cybersecurity efforts for over 12 years and have worked collaboratively with their industry and government partners in a number of areas, including coordinated cybersecurity efforts and information sharing. The intrusion and surveillance technologies addressed in the Department's proposed rules for implementing the Wassenaar Agreement represent a key component of their respective security measures.

In many instances, USTelecom members utilize a range of commercially available software engineering tools in their cybersecurity efforts. These tools include various third-party commercial products, including Core Impact, Burp and Metasploit, as well as software technologies and tools developed by individual companies. Such tools are widely utilized for remote management software, network vulnerability testing, antivirus and anti-intrusion testing.

As has already been widely acknowledged, many cybersecurity stakeholders – including USTelecom members – are currently seeing an increasing range of cyber threats emerging internationally. Because the Internet is a global network and cybersecurity is a global battle, USTelecom members engaged in defensive cybersecurity efforts need to identify – and ideally stop – such threats at the edge of the network before they traverse to networks within the United States.

Many USTelecom member companies have operations globally and have network security expertise distributed across countries. The Department's proposed license requirement for the "export, re-export, or transfer (in-country) of these cybersecurity items to all destinations, except Canada" would hobble the telecom's industry ability to react promptly and dynamically to the changing cybersecurity threats. International cooperation, including with foreign governmental entities, is indispensable to these efforts.

The Department's Proposed Rules Are Too Rigid

The Department's rules are too rigid, and will therefore hinder the ability of USTelecom's member companies to react to the rapidly changing cybersecurity threat landscape. USTelecom believes that in certain instances, the proposed rule could be interpreted broadly to control what many multi-national companies do today to monitor and manage their networks for security threats overseas.

For example, in the FAQ on the Department's website regarding intrusion and surveillance systems, the Department states that its proposed rule "would not control any 'intrusion software,' which may also be referred to as malware or exploits."³ However, in a separate question addressing whether the rules would cover companies monitoring overseas networks, the Department states that "systems, equipment, components or software that generate, operate or delivery or communicate" with "intrusion software" would require a license.⁴

Given the Departments definition of "intrusion software," a possible interpretation is that any network monitoring equipment or system is "communicating" with "intrusion software" and therefore could potentially be controlled.⁵ In addition, some USTelecom members have equipment today that extracts data from a network capable device, but it may be unclear as to whether such equipment is "specially designed...to avoid detection by monitoring tools or to defeat protective countermeasures."

Moreover, the Department's proposed rules will adversely impact the ability of USTelecom member companies to respond in a rapid and responsive manner. For example, in the course of responding to a cybersecurity attack or investigating a cybersecurity incident, malware samples and information about them that may constitute controlled technology may need to be rapidly shared across borders and with representatives of foreign governmental entities. Although the Department has indicated in its FAQs that intrusion software is not subject to the proposed controls, it would be a trivial matter for malicious developers of such software to enhance intrusion software to enable it to generate, operate, deliver, or communicate with itself and with other instances of such intrusion software. This highlights a fundamental flaw in the Department's approach—the assumption that "intrusion software" and the items sought to be controlled under ECCN 4D004 will in -fact remain different things. It is fully reasonable to expect malicious developers to modify their intrusion software going forward so that the intrusion software itself has the ability to "communicate" with intrusion software or generate new instances of it (self-replicating intrusion software).

³ See, Bureau of Industry and Security website, FAQs, Intrusion and Surveillance Items, Question 1 (available at: <https://www.bis.doc.gov/index.php/licensing/embassy-faq>) (visited July 6, 2015) (*BIS FAQ Website*).

⁴ *BIS FAQ Website*, Question 17.

⁵ The Department defines "intrusion software" as: "software 'specially designed' or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device, and performing any of the following: (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or (b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions."

Even if the malicious operators do not avail themselves of such features of their intrusion software, the existence of such features and capabilities may be sufficient to bring the intrusion software itself – the malware – within the ambit of U.S. export controls. At a minimum, the risk of this is likely to substantially burden cybersecurity-related information sharing of malware samples and related technology. To effectively impose a classification and licensing obligation through these rules for such activity – sharing of malware samples (*i.e.*, intrusion software) and information relating to their operation and design (*i.e.*, technology) – is a significant burden on cross-border, beneficial cybersecurity activity. In stark contrast, our industry’s cybersecurity adversaries face no such artificial administrative constructs and will not be so hindered.

Industry efforts could also be significantly hampered by dealing with the complexities of a licensing process. If a particular investigation in-fact involves software or technology controlled under the new rules, the possibility exists for ongoing reevaluation of licensing requirements at each twist and turn of the investigation, depending on the particular cybersecurity event’s origin and mix of impacted geographic regions. The nefarious users would not be hampered with having to deal with such a licensing agreement.

Given that cyber threats rapidly change, time is of the essence to get in front of these threats. The Department’s proposed rule that would require a license every time companies need to deploy new technologies or share cybersecurity related software and technology will be overly burdensome and create unnecessary and harmful delays. And the Department’s proposed rules will be nowhere near flexible enough to keep pace with the rapidly changing pace of intrusion software, the systems that control it, the use of such items in the online world, and the need to engage in the sharing and transferring of those items and related technology for cybersecurity purposes.

Need for Additional Comment

Given the rigidity of the regulatory process in such a dynamic area as cybersecurity, it is imperative that the Department ensure that all affected stakeholders have a meaningful opportunity to review the proposals and provide comments. In that regard, USTelecom recommends that the 30-day comment period be extended by at least 90 days or, in the alternative, that the proposed rules be reissued for comment later this year. This would likely be especially beneficial in light of the potential impact of these rules on the academic and research community, and the fact that the current 30-day comment period occurs exclusively outside of the academic year.

Recommended Changes to the Department’s Proposed Rules

In light of these realities, USTelecom proposes various changes to the Department’s proposed rules that balance the need for limited controls over certain technologies against the need for unhindered responsiveness by industry partners.

1. The Department Should Remain Cognizant of the Need for Innovation

As the Department considers its proposed rules, it should remain cognizant of the importance of, and need for, an environment favorable to innovation by industry stakeholders.

This is particularly the case given the unique nature of managed network services offered by many USTelecom members. As technologies evolve and industry services are developed and deployed, the Department should ensure that its rules did not create unnecessary burdens that may hamper such innovation.

Licensing frameworks that are overly inclusive may hamper the ability of industry stakeholders to pursue such beneficial innovation which is crucial to enhanced cybersecurity measures. Given the inherent flexibility of bad actors to rapidly adjust their own technologies and procedures, it is essential that industry stakeholders operating in the cybersecurity realm are afforded maximum flexibility in any regulatory scheme implemented by the Department. In addition, several countries with significant capabilities in cybersecurity are not party to Wassenaar, and their domestic cybersecurity industries will not be hampered by regulatory uncertainty regarding commercial development and exploitation of emerging cybersecurity technologies. It is imperative that the Department's rules not serve as a thumb on the scale against investment in cybersecurity innovation by U.S. companies, thereby shifting capital flows to investments in non-U.S.-based cybersecurity innovation and development.

USTelecom therefore encourages the Department to promulgate a default license exception that is as broad as possible, thereby allowing US companies to continue to innovate and develop tools in the dynamic and fast-moving cybersecurity environment. Such a license exception could be based on the provision set forth in License Exception ENC,⁶ and could take the form the license exception example included as Attachment A to these comments. At a minimum, this new exception should apply to all items proposed for control under Category 4.

USTelecom proposes that such an exception would be consistent with policies currently underpinning License Exception ENC, pursuant to which many of these items are now exported today. In particular, a framework modeled on License Exception ENC provides a framework that is already familiar to industry stakeholders. The existing License Exception ENC framework provides a roadmap that is both efficient and familiar to industry stakeholders, thereby ensuring rapid development, marketing and distribution of such tools. In addition, USTelecom submits that the continued export of such items subsidiaries of US companies would continue to balance US Government foreign policy and national security interests. US subsidiaries are more likely to utilize such items for defensive, rather than offensive, purposes. And finally, treating Category 4 cybersecurity items in a manner consistent with encryption items from a licensing exception perspective would be consistent with how USTelecom understands these controls were implemented in the European Union countries.

2. Cybersecurity Licensing Exception.

In addition to adding the licensing exception along the lines proposed above, USTelecom recommends a new "cybersecurity exception" for items controlled under Category 4. This new exception would eliminate any licensing requirement for the export, re-export, or in-country

⁶ Section 740.17(a)(2), Export Administration Regulations.

transfer of software and technology controlled under those ECCNs. This proposed exception would relieve US companies of the burden of attempting to classify malware samples and of seeking licenses for sharing such samples and information about their development, operation, use, and other features in the context of information sharing and cybersecurity activities.

The exception would be applicable where: (a) the software or technology was identified, obtained, or developed in the context of defensive cybersecurity activity; (b) the software was not developed by and not a product of the entity that identified it; and (c) the export, re-export, or in-country transfer took place in the context of legitimate cybersecurity preventative, investigative or responsive activities.

3. Explanatory Note to Include Carve-Out for Enterprise Cybersecurity Activities

Turning to items proposed for control under Category 5 related to Internet Protocol (IP) network communications surveillance systems, the Department has advised that the “term ‘carrier class IP network’ is meant to specify systems that sit at a national level (or large regional) IP backbone and handle data from an entire city or country.”⁷ In terms of IP network surveillance systems, this is meant to exclude systems that can only handle smaller data streams or networks, such as those for a campus or a neighborhood.

This control does not capture systems that can only analyze data from one person or a small group of people at a time. The term ‘carrier class IP network’ was not defined because it was “difficult to put precise technical parameters around this concept.”⁸

Notably, the proposed regulations exclude from the proposed controls any such items that are used for “marketing” purposes, network quality of service, and quality of experience. USTelecom recommends that this list of exclusions in the explanatory note accompanying 5A001.j be expanded to include “enterprise security.” Today, enterprises including USTelecom members may deploy systems specially designed with the capabilities described in 5A001.j not only for service delivery (and in limited instances, with appropriate privacy protections, marketing purposes), as contemplated by the existing “Note,” but also for enterprise security. Such systems can be very beneficial in identifying a range of potential insider threats such as loss of proprietary information, misuse of system privileges, and potential sabotage, and are typically employed at the level of a company’s proprietary corporate network.

Conclusion

USTelecom appreciates the Department’s consideration of our comments in this proceeding. In closing, USTelecom also requests that if the Department intends to proceed with new rules in this area, irrespective of the content of those rules that the Department provide for a six-month implementation period. Many USTelecom members operate globally in multiple

⁷ *BIS FAQ Website*, Question 14.

⁸ *Id.*

U.S. Department of Commerce

July 20, 2015

Page 7

countries, and employ security engineers and technicians from other countries. Restructuring existing managed security service delivery arrangements, staffing arrangements and other cybersecurity activities affected by the new rules will take a significant amount of time.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert L. Mayer". The signature is fluid and cursive, with the first name "Robert" being the most prominent.

Robert Mayer
Vice President, Industry and
State Affairs

Attachment A

License Exception XXX authorizes export, re-export and retransfer of cybersecurity systems, equipment, and components therefor classified under ECCNs 4A005 or 5A001.j; cybersecurity telecommunication test, inspection and production equipment, “components” and “accessories” classified under ECCN 5B001 (if for 5A001.j); equivalent or related software classified under ECCNs 4D001.a (if “specially designed” or modified for 4A005 or 4D004), 4D004 or 5D001 (if “specially designed” or modified for 5A001.j or 5B001.a); and technology classified as 4E001.a (if “required” or modified for 4A005, 4D001.a or 4D004 cybersecurity items) or 5E001 (if “required” or modified for 5A001.j, 5B001.a or 5D001.a cybersecurity items) to any “U.S. subsidiary,” wherever located without a license. License Exception XXX also authorizes export or reexport of such items by a U.S. company and its subsidiaries to foreign nationals, except nationals of Country Group E:1 in Supplement No. 1 to part 740 of the EAR , who are employees, contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use, including the “development” or “production” of new products , without a license.

PUBLIC SUBMISSION

As of: 7/29/15 6:15 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-6t6o
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0259

StrategicIO Kyle Hanslovan

Submitter Information

General Comment

See attached

Attachments

StrategicIO Kyle Hanslovan

July 20, 2015

To: Office of Exporter Services
Bureau of Industry and Security
U.S. Department of Commerce
14th and Pennsylvania Ave. NW.
Washington, DC 20230

Attn: Sharron Cook
publiccomments@bis.docs.gov

**RE: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items
RIN 0694-AG49 / BIS-2015-0011**

Thank you for the opportunity to submit comments regarding Regulation Identifier Number 0694-AG94. StrategicIO, LLC is a defense contracting firm based in Ellicott City, Maryland. We support US Intelligence, Military, and Law Enforcement communities with the development of offensive cyber capabilities. With this experience, we consider ourselves subject matter experts regarding technology specially designed for the generation, operation or delivery of, or communication with intrusion software. Although our company does not currently engage in commerce which would require additional export licenses under the Proposed Rule, we have not excluded this possibility.

StrategicIO is familiar with the Wassenaar Arrangement (WA), Export Administration Regulations, Arms Export Control Act, and International Traffic in Arms Regulations and is registered with the Directorate of Defense Trade Controls under code M35086. We've read all BIS publications under Docket ID BIS-2015-0011 and understand the intent to control the export of cybersecurity technologies for the purpose of fulfilling U.S. obligations under the WA. With this in mind, our response will focus on our concerns, redundancies, and shortcomings of the currently proposed U.S. implementation.

StrategicIO requests that BIS consider conducting an independent value proposition assessment to determine the effectiveness of the proposed cybersecurity controls vs. the existing controls afforded by Category 5 part 2 of the EAR.

As indicated within RIN 0694-AG49 Rulemaking Requirements paragraph 2, BIS already acknowledges "most of the items impacted by this rule have encryption capabilities" and "believes they are already being controlled." Considering the speed at which technology changes, a further investigation outside of the public request for comments should be conducted to ensure this redundancy doesn't inadvertently impact commerce opportunities which have not been recognized. It is our opinion that redundant reviews for Encryption Items and Intrusion and Surveillance Items will negatively impact the agility of small businesses to demonstrate product functionality and conduct business in a timely manner. Additionally, we believe the existing encryption controls adequately prevent acquisition by countries which fall under regional stability concern.

Considering BIS' previously quoted acknowledgments, it's reasonable to conclude the Proposed Rule only affords additional control to encryption-free intrusion software. Considering recent Government outcry against encryption and its ability to hinder law enforcement activities, it seems counterintuitive to put additional scrutiny on easily monitored software which may have intelligence value.

Should the Proposed Rule co-govern with the existing encryption export controls:

StrategicIO requests that BIS removes references to rootkit technologies and zero-day exploits.

The definition of intrusion software and FAQ Responses #1, #2, #4, #7, #11, #12, and #15 adequately describes command and control platforms used for generation, operation, delivery, and communication with said intrusion software. A presumptive denial for items which support these capabilities is unneeded as the Proposed Rule already references technology for the development or production of command and distribution or intrusion software. The presumptive denial also fails to consider the ramifications to cyber defenders responsible for protecting against network intrusions who would leverage properly licensed rootkit technologies and zero-day exploits for training purposes.

Additionally, the referenced FAQ Responses should be incorporated back into the Proposed Rule as technical notes to correct the unorthodox legal approach taken by BIS to clarify shortcomings of the original proposal. Although the FAQ was extremely useful to gain insight on BIS' perspective, the document is not legally binding.

StrategicIO requests that BIS expand exceptions for license requirements and countries to receive favorable treatment for license applications.

Considering the close economic and cybersecurity policy relationships, exceptions for license requirements should be expanded to Australia, New Zealand, and the United Kingdom. These close allies maintain the same exceptional human rights record as Canada and should not be treated as second class citizens when it comes to the global cybersecurity market. Additionally, favorable treatment should be expanded to NATO allies to help offset the likely impact incurred with the loss of ENC license exceptions.

Thank for reviewing our feedback and we look forward to seeing how BIS addresses our above outlined concerns.

Respectively,

The StrategicIO Team

PUBLIC SUBMISSION

As of: 7/29/15 6:16 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-mnmz
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0260

steptoe Kaitlin Cassel 7-29

Submitter Information

General Comment

See attached

Attachments

steptoe Kaitlin Cassel 7-29

Meredith Rathbone
202 429 6437
mrathbone@steptoe.com



1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

July 20, 2015

Via e-mail

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20230
publiccomments@bis.doc.gov

Attn: Catherine Wheeler, Director, Information Technology Controls Division

**Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation:
Intrusion and Surveillance Items**

**Reference: BIS-2015-0011
RIN 0694-AG49**

Dear Ms. Wheeler:

These comments are submitted on behalf of the Coalition for Responsible Cybersecurity (the "Coalition") to express the Coalition's concerns with the BIS proposed rule *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28,853 (May 20, 2015) ("the proposed rule"). The Coalition's mission is to ensure that U.S. export control regulations do not negatively impact the effectiveness of U.S. cybersecurity or prevent the United States from maintaining its leadership role in that sector. The Coalition is representative of a broad range of companies, and includes Ionic Security Inc., Symantec Corporation, FireEye, Inc., Synack, Inc., Trail of Bits, Inc., Global Velocity, Inc., and WhiteHat Security.

U.S. companies design, test, develop, and field some of the world's leading technologies in critical areas such as network monitoring, penetration testing and encryption. Development of these cutting-edge defensive technologies relies on the ability to conduct unfettered research into vulnerabilities (including novel, zero-day vulnerabilities), as well as reverse engineering cyber threats and other basic methods of cybersecurity research. However, robust research and

development are only feasible when there is an open, global market for the products. If U.S.-origin technology becomes “tainted” by burdensome export control restrictions, U.S. companies will lose their leadership position, to the detriment of all the companies, organizations, governments and individuals that rely on U.S. cybersecurity to defend against malicious attacks.

U.S. companies “export” these defensive technologies virtually every second of every day. Imposing the far-reaching licensing requirements that BIS has proposed would harm not only U.S. cybersecurity companies, but would harm cybersecurity itself. The Coalition is committed to helping the U.S. government ensure that its export control regulations are informed by the realities of the cybersecurity world and do not inadvertently restrict beneficial activity or miss the mark in attempting to control malicious activity. It is also important that U.S. export controls remain in line with, and not needlessly more restrictive than, those of its major trading partners and technological competitors. Otherwise, U.S. cybersecurity leadership and expertise will weaken, causing the United States to lose its strategic edge and its world-leading contributions to this arena, while the cybersecurity markets continue to strengthen in countries that are not subject to such harsh restrictions.

The Coalition has done its best to craft useful and detailed comments in the short period of time that BIS has allowed. However, the Coalition is unable to raise all of the concerns implicated by this sweeping regulation in this initial round of comments. Due to the complicated nature of this proposed rule and its effects on industry, the Coalition believes that a second proposed rule and round of comments is necessary. The current proposed rule as drafted would have a devastating effect on U.S. cybersecurity and must be fundamentally restructured. We discuss in more detail in Section VII.A.3, below, what a productive subsequent proposed rule might look like.

I. INTRODUCTION

The proposed rule would achieve the exact opposite of what the Wassenaar group intended: rather than effectively restricting trade in malicious items, it will primarily control the defensive technologies that law-abiding organizations rely on to protect themselves against those malicious items. Many of the Coalition’s concerns with the proposed rule focus on its use of ambiguous language and overbroad definitions that capture defensive tools and standard software development techniques that apply even outside the security sphere. In its Frequently Asked Questions (“FAQs”) on the proposed rule, BIS itself expressed the difficulty it faced in defining some of the terms, such as “carrier class”.¹ Terms like “rootkit” and “zero-day” are used in the proposed rule with no definitions, even though they have more than one accepted meaning in the cybersecurity community. The definitions that are provided, such as for “intrusion software,” are overbroad and unworkable. They cover a wide range of cybersecurity products that BIS likely did not intend to target.

¹ See, e.g., BIS, Frequently Asked Questions, Intrusion and Surveillance Items (“FAQs”) #14, <https://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>.

BIS itself has recognized that the proposed rule captures some defensive products and methods, such as network penetration testing.² That the proposed rule captures penetration testing should not be taken lightly. Penetration testing is a standard operational need to maintain the security of electronic systems; in fact, penetration testing is required by numerous industry standards and regulations.³ As currently written, the rule would cover numerous other defensive products in addition to penetration testing, because the products security professionals use to add new security features and patches are frequently technically indistinguishable from those used by attackers to alter programs in malicious ways. There are very few characteristics or behaviors that can even be potentially considered unique to malicious tools, and even screening for these malicious characteristics often brings up false positives for security software, demonstrating that there are probably no characteristics that are exclusively malicious. While BIS has recognized the difficulty of distinguishing between offensive and defensive products, it has not succeeded in implementing an effective distinction. That is a critical shortcoming that calls for more time to allow the government to consider how to craft a regulation in this area that would achieve its stated objectives without unnecessary collateral damage. Again, we provide some preliminary suggestions for how to get started on this effort in Section VII.A.3, below.

The proposed rule makes no effort to distinguish between items that assist in interfering with or extracting data from *malicious* programs (in order to defend against them) and those that maliciously interfere with *legitimate* programs (as a means of attack). Many security tools use technology that implements, executes, or monitors malware and extracts data from that malware for defensive purposes. Such tools need reliable ways to be generated, operated, and delivered, all of which would be unduly restricted under the proposed rule. Similarly, many benign products meant to patch systems or programs, or add capabilities that the authors did not originally contemplate, do so by interacting with and manipulating the program in ways that would be captured under the proposed definition of “intrusion software.” The cybersecurity community is global and their defensive efforts occur in real time and often depend on collaboration across borders. These controls would greatly complicate these collaborative efforts and access to legitimate software tools. But the proposed rule is unlikely to stop malicious actors from sharing and using their products because these actors often operate outside the reach of U.S. regulatory power. Additionally, even though other Wassenaar countries have used much of the same overbroad and fundamentally problematic language from the December 2013 plenary, this proposed rule controls an even wider range of items than Wassenaar and other countries’ implementing rules, including differences in the implementation of the General Software Note and General Technology Note.

² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28,854 (stating that the new controls will “include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices”).

³ See, e.g., Federal Information Security Management Act (FISMA) of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3544(b)(5); see also *Technical Guide to Information Security Testing and Assessment*, U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-115 (September 2008); *Penetration Test Guidance*, Federal Risk and Authorization Management Program (FedRAMP), Version 1.0.1 (July 6, 2015). See generally, Section V, below.

From an overall perspective, the proposed rule is unworkable because the language that was adopted in December 2013 by Wassenaar is fundamentally flawed. Ideally, rather than try to adopt this language through regulation in a sweeping and harmful way, the U.S. must return to Wassenaar to change this language. Because of the unique nature of the cybersecurity industry, which depends on rapid information sharing among an international community of professionals, no traditional export control licensing policies can solve the fundamental problems in the proposed rule. These issues likely stem from the adoption of the Wassenaar language without any industry input. Tellingly, the overwhelming majority of the cybersecurity industry is in the United States, while the Wassenaar rule was proposed by a European country without seeking feedback from U.S. industry. Now that U.S. industry's input is being heard, it is unfortunately—but inescapably—necessary to go back to the drawing board. Given the likely timeline for revisiting this issue at Wassenaar, and the timeline for a second notice and comment period, we believe that returning to Wassenaar will not significantly delay the United States' implementation of a cybersecurity rule. Specifically, due to the significant problems with the current proposal, and the need for a second round of comments to get industry input on any revisions, this rule is unlikely to be anywhere near finalization by February 2016, when the U.S. government needs to send its proposals for changes to Europe for the 2016 Wassenaar meeting. Indeed, the best use of industry's comments on the proposed rule may be to begin flagging a series of critical issues for the United States at early meetings related to Wassenaar before February, rather than trying to rush a final rule to completion. For that reason alone, the time spent in getting this rule right, not only for the United States but for other Wassenaar countries, is a worthwhile investment of time.

In the sections that follow, the Coalition lays out its key concerns with each part of the proposed rule. It then discusses the inconsistencies with Wassenaar and several countries' implementation of that agreement, as well as with data security requirements in other industries and the U.S. government's own information sharing and security initiatives. Next, it looks at the consequences of the proposed rule, which would have a dire impact on cybersecurity in the United States. Finally, it offers a number of preliminary proposals to begin to help BIS develop a framework that might accomplish its goals, while also protecting critical cybersecurity products and methods.

II. CONCERNS WITH PROPOSED CONTROLS

The Coalition has serious concerns with the ambiguous and overbroad language used in the proposed rule, which would capture not only cybersecurity products, but also basic software development techniques more generally.

A. Effective Control of "Intrusion Software"

Intrusion software would be effectively controlled by the proposed rule, despite the stated intent of BIS to the contrary. The FAQs released by BIS on intrusion and surveillance items emphasize that "intrusion software" is not itself controlled, so the transfer of exploit samples, proofs of concept, and other forms of malware are not controlled.⁴ But it is not possible to

⁴ See, e.g., FAQs #1, #2, #10, #19, and #24.

effectively share vulnerabilities and exploits for defensive purposes, or to use defensive “intrusion software,” without using control and delivery platforms and sharing the equipment, software, and/or technology behind them. While there is ostensibly no direct control of “intrusion software” itself, as a practical matter, the controls are broad enough to effectively control intrusion software by controlling items that generate, operate, deliver or communicate with it, and technology for the development, production or use of such items.

Vulnerability testing and patching is a good example of how the proposed rule would effectively control intrusion software. BIS states in FAQ #12 that vulnerability scanners, which find potential vulnerabilities in a system without actually exploiting them and extracting data, would not be captured. But this ignores the reality of the process of vulnerability research, which is not about just finding potential vulnerabilities or even sharing proofs of concept. When finding vulnerabilities and reporting them, the most valuable information to share with a vendor to help develop a patch is the information on how the vulnerability can be exploited and how the exploits work, including the technology used to develop them. This helps the vendor understand the root cause of the vulnerability and develop a more complete and long-lasting defense instead of just a “band aid” fix.⁵ Then, in FAQs #10 and #19, BIS recognizes that controlled “technology” may be transferred during the reporting of a vulnerability or exploit, highlighting that this process will indeed be subject to these highly restrictive controls. And in FAQ # 13, BIS recognizes that the tools used to test vulnerabilities (which find vulnerabilities and extract data to prove the vulnerability is real) would meet the technical description of items controlled under ECCN 4A005 and 4D004. If BIS were to control the information flow about exploits, as it has proposed in this rule, it would have profound effects on companies’ ability to produce successful defenses.

Similarly, third parties often make “exploits” to provide update services and manual patching for commonly-used software products produced by other companies. Such third party participation is necessary to supplement the features offered by the original provider, or where that original provider has gone out of business or has stopped supporting its code, as is often the case for critical infrastructure. Unlike auto-updaters that are part of the original software, these third parties use “exploits” to deliver updates and patches into vulnerable programs and systems.⁶

⁵ While an exploit on its own is not sufficient for defensive purposes, as understanding the root cause of the vulnerability is necessary to create an effective defense, for *offensive* purposes a single sample of malware may indeed be enough—especially considering that often general purpose tools, which would likely not be captured by this proposal, can be used to deliver and communicate with it. *See generally*, Section VI.D. Thus, while this attempted distinction in the proposed rule hurts defensive efforts, it likely does little to stop the export of malware for malicious use.

⁶ *See, e.g.*, Collin Mulliner et al., *PatchDroid: Scalable Third-Party Security Patches for Android Devices*, <https://www.mulliner.org/collin/publications/patchdroid.pdf> (describing “PatchDroid, a system to distribute and apply third-party security patches for Android” because many Androids contain “known security vulnerabilities [that] cannot be updated through normal mechanisms since they are not longer supported by the manufacturer and mobile operator”). Another example is the Xen hypervisor used by Amazon Web Services (“AWS”). While the Xen hypervisor is open source, AWS uses a customized version that is not public. Sometimes

They use these “exploits” to defeat the integrity of the original system, bypassing its protective measures, modifying its standard execution path, and providing external instructions. Even if the “exploits” themselves are not controlled, the related controls appear to squarely capture parts of these update and patching tools that deliver and communicate with the components that actually apply the patch.

BIS should recognize that any items that are captured by the definition of “intrusion software” will be effectively controlled by the proposed rule. Products need tools to deliver and communicate with them in order to be useful and marketable. Additionally, companies need to communicate in detail about vulnerability reports with vendors to create an effective patch. Therefore, control of these delivery, control, and communication mechanisms, as well as technology for their development, production and use, acts as an effective control on defensive products qualifying as “intrusion software,” as well as on sharing vulnerabilities and exploits.

B. Overbroad Definition of “Intrusion Software”

The effective control of all “intrusion software,” as well as related systems, software, and technology, would be particularly damaging given how broadly that term is defined, encompassing tools and products that are purely defensive. Below we discuss each aspect of the definition.

1. Software specially designed or modified to avoid detection by “monitoring tools” or to defeat “protective countermeasures” of a computer or network-capable device

This first part of the definition of “intrusion software” is ambiguous in numerous respects, in a way that makes its scope overbroad.

a) “Avoid detection” and “defeat”

The terms “avoid detection” and “defeat” are unclear. For example, in its FAQ #8, BIS states that auto-updaters are not controlled because, while they “may need to interact” with monitoring tools and protective countermeasures, they are not “defeating” or “subverting” the system. However, the line between merely “interacting” and “avoiding detection” or “defeating” is not clear. The reason for this “interaction” is so the monitoring tools and protective countermeasures allow the update to occur uninterrupted, which could reasonably be interpreted as “avoiding detection” or “defeating” such measures. The drafters seem to be contemplating a distinction in the proposed rule between permitted interactions that defeat existing monitoring and protections and those with the same effect that do not have permission. But they did not make such a distinction in the proposed language. Moreover, it would not even be clear whose

this version needs to be patched for security vulnerabilities, and AWS must push these patches across the globe at an urgent rate. These patches are made by AWS itself, not Xen—and they are delivered worldwide before the security vulnerability is made public. *See* Brandon Butler, *What happens inside Amazon when there’s a Xen vulnerability*, NETWORK WORLD (Mar. 3, 2015), <http://www.networkworld.com/article/2892313/cloud-computing/what-happens-inside-amazon-when-there-s-a-xen-vulnerability.html>.

permission would matter. The user? The network owner? The author of the software? There are legitimate software updates that occur without the permission or even the knowledge of the user or owner, and others that occur without the permission or even the knowledge of the author of the original software.⁷ This is a complex problem that the proposed rule has not taken into account.

b) “Monitoring tools”

The scope of the term “monitoring tools” is unclear, and guidance from BIS has raised the additional question of whether it intends to exclude all monitoring tools from the definition of “intrusion software.” For example, BIS states in its FAQs that “anti-virus software” is explicitly excluded from the definition of “intrusion software” because it is a “monitoring tool.”⁸ However, BIS does not make any such broader exclusion explicit, raising serious doubts about the scope of the proposed rule. Simply because “avoid[ing] detection by monitoring tools” is part of the “intrusion software” definition, it is not obvious that a “monitoring tool” cannot also be “intrusion software.” For example, antivirus software itself could be classified as “intrusion software” because it modifies the standard execution path of software to intercept and inspect data passing through the network to ensure that malicious actors are not exploiting the software. And it often has rootkit capabilities—it operates under the user interface and subverts part of the operating system so that when a program or user takes an action, it can intercept the action, inspect it, and, if necessary, modify the result with or without the user’s knowledge. BIS has labeled this “rootkit” capability presumptively offensive; however, these capabilities are necessary for antivirus software because they are the only means of getting inside a system at a deep enough level at which they can effectively monitor for and catch malicious traffic before it can infect the system.

Neither “monitoring tool” nor “antivirus software” is included among the explicit exceptions in the proposed rule.⁹ It is therefore not clear whether BIS meant in its FAQ #8 that *all* monitoring tools that are also intrusion software are excluded or whether antivirus software is somehow distinct. There are plenty of examples of products, in addition to antivirus software, that can be both “intrusion software” and a “monitoring tool”—including some that can be used for both benign and malicious purposes. Take keyloggers, which have traditionally been seen as malicious malware that records keystrokes to steal information. But keyloggers are certainly

⁷ See, e.g., *supra*, Section II.A (discussing third party updaters who provide updates and patches where companies have gone out of business or stopped supporting their code); and *infra*, Section II.B.2.c (discussing software innovation and development of third-party software to be used with other companies’ software products, both of which often require modifying the standard execution path of a program or process without the knowledge of the original designer).

⁸ See FAQ #8.

⁹ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28858 (May 20, 2015) (“Intrusion software” does not include any of the following: a. Hypervisors, debuggers, or Software Reverse Engineering (SRE) tools; b. Digital Rights Management (DRM) “software”; or c. “Software” designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.”).

“monitoring tools,” although BIS presumably would not want to exclude them from the definition of “intrusion software.” This is just an example of how difficult it will be to draw lines effectively in this industry.

Even “monitoring tools” with a traditionally nefarious reputation have legitimate uses, such as endpoint security products that allow companies to monitor their networks or particular employees.¹⁰ These products, just like malicious keyloggers, extract user data. Both are “monitoring tools,” but also come within the definition of “intrusion software” (and often even have “rootkit” capabilities¹¹). The key difference is the intent of the customer and the authorization of the system administrator.

These examples show the importance of clearly defining “monitoring tools” and explicitly stating under what circumstances a product would be excluded from the definition of “intrusion software” where it may fit the definition of both (and could even have malicious uses).

c) “Protective Countermeasures”

The term “protective countermeasures” suffers from the same lack of clarity as “monitoring tools.” First, the uncertainty over whether there is an exception for “monitoring tools” raises the question of whether “protective countermeasures” are also excluded. Second, the language of the proposed rule does not make any distinction between defeating the “protective countermeasures” of *legitimate* systems and defeating the “protective countermeasures” that protect *malware*. Because of this shortcoming, a product aimed at defeating the protective countermeasures of malware, in order to defeat the malware, would fall within the scope of the rule.

Third, despite the short definition provided in the proposed rule, it is not clear what a “protective countermeasure” must protect in order to qualify as one. While the examples in the proposed rules emphasize Data Execution Prevention (“DEP”), Address Space Layout Randomization (“ASLR”) and sandboxing, which ensure the safe execution of code to protect the system and user, Digital Rights Management (“DRM”) software also often allows for the “safe execution of code,” but it does not protect the interests of the user; it protects the intellectual property of a third party. Would DRM be considered a protective countermeasure? Would defeating DRM software or “jailbreaking” a phone be considered defeating “protective countermeasures”? BIS seems to accept that it would be in FAQ #26, but without a detailed definition, the scope of “protective countermeasures” remains uncertain.

¹⁰ See, e.g. Bodi, Pilixo, <https://www.pilixo.com/resources/lp/computer-monitoring>; Computer & Mobile Monitoring Software, Webwatcher, <http://www.webwatcher.com/pc-monitoring>.

¹¹ For example, as can be seen in the websites in footnote 10, these “monitoring tools” are advertised for their “undetectable” and “tamper proof” methods, including hiding their processes from the monitored users and any antivirus software they may install.

d) “Network-capable device”

By including mobile devices and smart meters in the definition of “network-capable device,” BIS would introduce potential liability for mobile device users and other consumers that have no control over products that may be embedded without their knowledge. For example, if the rule is interpreted to cover both sides of a “communication” with malware (both the “controller” side used by the attacker and the “receiver” side on the hacked device), the owner of a phone that has been hacked and contains malware may violate the rule by taking the phone abroad without a license. While such an unwitting victim would not have had any intent to violate the controls, the EAR impose strict liability.

2. Performing any of the following: (a) Extraction of data or information, from a computer or network-capable device, or the modification of system or user data or (b) modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions

The second part of the definition of “intrusion software”—the requirement that it extract or modify data or modify the standard execution path of a program—captures a wide swath of legitimate programs.

BIS’s attempts to limit the definition leave many open questions. For example, in FAQ #11, BIS states that “[o]ther types of malware, including software that only leaves evidence of a successful security breach without further compromising or controlling the system” are not included. However, it is difficult to see how a program can leave evidence of a security breach without modifying the standard execution path of the program, executing externally provided instruction, and possibly modifying some data. Creating evidence of a security breach is not within the normal scope of software operation (normal working systems do not have a built in button that says “click here to show a breach”). The program “leaves evidence” of such breaches by changing the behavior of the system (modifying the standard execution path) and typically also modifying data to leave the trace (the equivalent of a note, “I was here.”).

While the concept of extracting or modifying data may be understandable, though very broad, there is no attempt to define “standard execution path of a program or process” and the potential breadth of what “modifies” such a path may capture a wide array of products. BIS has clarified that this language is meant to refer to a variety of techniques used to hijack, or otherwise corrupt, a legitimate (or otherwise trusted) application or process running on a computer, mobile phone, or other device.¹² It continues that this can be done for persistence or for other purposes, and that through these modifications, a remote operator (or remote command and control software) can execute commands or perform other tasks that further compromise or exploit the hacked (penetrated) device.¹³ However, there are problems even with this attempted clarification, which appears to define modifying a standard execution path as doing anything with a program or process that the original author did not intend. Again, without saying so, the essence of these controls appears to boil down to a question of intent. But if intent is what BIS meant, the definition needs to be more specific. A reasonable person could interpret “standard”

¹² See FAQ #30.

¹³ See FAQ #30.

to simply mean “default” or the path used the majority of the time. And if “intent” is what is necessary, the definition needs to be clear about whose intent matters (for example, it could be the network owner, the system user, the system administrator, or the developer of the software; and do these persons need to have predicted the exact modification that occurs, or is it enough that they intended some path modifications to occur?). Additionally, as discussed elsewhere in these comments, often legitimate computer programs change existing software—for the better—in a way that the original author did not intend or predict.

a) *No distinction between interfering with legitimate systems and processes and malicious ones*

Whereas FAQ #30 emphasizes hijacking or corrupting *legitimate* and *trusted* applications or processes, the language in the proposed rule itself does not make any distinction between hijacking and corrupting legitimate applications versus malicious ones.¹⁴ As written, the proposed language would apply to software meant to extract or modify the data of *malware* or to modify the standard execution path of *malicious* programs and processes (i.e. to defeat them).

For example, the rule would appear to capture malware recovery tools, which are used to regain control of a system infected by malware. When a user has lost control of its system to malware, the malware does not simply have an off switch to uninstall it. Instead, the malware will often put protective countermeasures in place to stop a user from uninstalling it, leading to a need for defensive tools that use exploitation (i.e. “intrusion software”). And such tools must be generated, operated, delivered, and communicated with in order to run effectively on the compromised system and defeat the malware.

A well-known example of such a protective tool is CISCO’s Talos TeslaCrypt Decryptor.¹⁵ This “decryptor” was developed to deal with a particular type of ransomware (a “cryptolocker”) that works by taking a system user’s valuable files (targeting photos, videos and documents) and encrypting them, after which a user has to pay a “ransom” to get them back. As a defense against this ransomware, CISCO released an “exploit,” its decryption tool, as well as the tools to run and deliver it. The tool works by defeating the protective countermeasures of the infected system to get at the malware, as well as the protective countermeasures of the malware itself; it then both (1) modifies the standard execution path of the malware to provide external instructions to interrupt and regain control of the system and (2) extracts data from the malware (to obtain the encryption keys) and from the infected system (to recover the encrypted files). In order to be practically used by average users, it has to be delivered to the computer together with

¹⁴ Additionally, even if the rule did explicitly make a distinction between “legitimate” and “non-legitimate” uses, this would be very difficult, if not impossible to determine in a technical sense. It would seem as though it would need to be based on someone’s approval (whether the network owner, system administrator, or authorized user of the software), but even this definition could run into problems if the approvals and knowledge of these actors conflict.

¹⁵ See Andrea Allievi, Earl Carter & Emmanuel Tacheau, *Threat Spotlight: TeslaCrypt – Decrypt it Yourself*, CISCO BLOGS (Apr. 27, 2015), <http://blogs.cisco.com/security/talos/teslacrypt>.

the tools to operate and communicate with it. As such, it would fall squarely within the definition of “intrusion software” and ECCN 4D004.¹⁶

This class of “exploits” and “intrusion software” has the explicit purpose of protecting users from other malware. Other legitimate tools—rootkit and virus uninstallers, adware removal suites, and ransomware remediation—act similarly to recognize, interrupt, and stop malware, and may be similarly covered.

b) Legitimate reasons to extract and modify data from or alter a standard execution path of a trusted system or process

There are legitimate defensive reasons to extract and modify data from or alter the standard execution path of trusted systems and processes. For example, the products of Ionic Security Inc. (“Ionic”) add additional security to legitimate programs, which the original program’s author did not contemplate and may not know about. Ionic’s products protect individual pieces of data, including those entered into cloud or desktop applications, so the data remains protected wherever it goes and to whomever it goes. It also allows the document owner to alter the access to their data remotely and retain control over access even after the data has left their physical control—a method of security that is of increasing importance with growing cloud computing and other trends. But, the products appear to be caught under the definition of “intrusion software” (and thus the controlling ECCNs as well). To secure this data, these products must alter the standard execution path of legitimate programs in ways that allow for the execution of externally provided instructions; and they must have equipment and software which operate, deliver, and communicate with them.

For example, to protect data entered into a network, Ionic uses a plug-in, through which data can be encrypted as it is entered.¹⁷ Unencrypted data never leaves the network, and the controlling keys to unencrypt the data remain with its creator. To do this, the plug-in must interrupt the flow of data; in essence, it diverts control of the program as the user sends data to use Ionic’s logic instead of the program’s standard path. This process requires the plug-in to interrupt the standard execution path of the program on which the data was created or stored, and extract and modify the data entered by the user, thus meeting both parts of this element of the

¹⁶ These malware recovery tools are also discussed briefly below for their ability to “communicate” with the ransomware, another reason they would be covered by ECCNs 4A005 and 4D004.

¹⁷ Currently, Ionic’s “plug-ins” for network content protection work with built-in plug-in architectures. In these situations, the original developer contemplated and intended plug-ins to be used to make changes or additions to the program. While these “intended” changes may not have been meant to be caught by the proposed rule, as discussed above, this is not entirely clear in the current language. For example, a reasonable interpretation of “standard” could be the “default” path, which plug-ins alter, even if alternative “execution paths” were contemplated in its original design. If “standard” was meant to convey a distinction of intent or authorization, such a distinction should be more clear; also, it would need to be specified whose intent or authorization is necessary (the original program designer? the user of the computer? the system administrator? the network owner? all of the above?).

definition of “intrusion software.” The plug-in receives a configuration that allows it to behave differently depending on the website being accessed, since different websites will require different methods to control and protect data. This also modifies the standard execution path of the websites in order to allow the execution of externally provided instructions regarding the protected data. To work effectively, such programs must also avoid monitoring programs, in order to provide a seamless interface and not set off antivirus software—thus meeting all elements of the proposed rule’s “intrusion software” definition.

A similar functionality of Ionic’s products can provide protection for individual pieces of data in a document, which the creator can set to different levels of access (public data, restricted data, etc.). To do this, the product makes modifications to the document and word processing software through a plug-in;¹⁸ the plug-in inserts itself into the software and interrupts the software’s processes. For example, to allow the user to save the document with Ionic’s encryption protections, the Ionic plug-in must interrupt the standard software program’s “save” workflow and instead instructs the system to use Ionic’s workflow. This involves hooking into the software’s standard code and modifying it to change how the document is saved, so that the document can be secured. And it is not necessarily done with the permission of the original software developer. This capability—to divert the behavior of the program to act differently than how it was meant to work (diverting the flow of the program to use the Ionic product’s code instead of its own)—seems to clearly qualify as modifying the standard execution path of a program, as well as extracting and modifying data; and it is again done to avoid setting off protective countermeasures or monitoring programs. Such program manipulation is necessary to make the security feature user-friendly and effective. And both its use (which requires tools to deliver, operate, and communicate with it—which include capabilities that Ionic needs to “export” to foreign customers) and development will be controlled under the proposed rule.

Various other functions of Ionic’s products also appear to be captured in the “intrusion software” definition. For example, in addition to providing encryption which follows individual pieces of data and allowing for remote changes to the data’s access controls, Ionic allows users to keep track of how and where their data is accessed, even once it has left their network. The plug-in extracts data from the system every time access to a protected item is requested to allow the policy services to decide if the data access should be granted. Such extraction of data again appears to fall within the definition of “intrusion software.”

Yet another example are the products Ionic offers to assist highly regulated industries with their compliance responsibilities. For example, some regulated industries, such as the financial services industry, are required to store their electronic communications for possible audits. However, due to web applications, such as Facebook and LinkedIn, businesses face compliance problems where their employees use such web applications to communicate in a way that is not recorded or logged. Ionic has worked to create an innovative solution to block certain features of these web applications (such as the messaging and posting features) on authorized

¹⁸ Unlike the network plug-ins discussed above, Ionic’s plug-ins that work with desktop software often work outside and go further than the software’s built-in “plug-in” architecture (if any exists) intended. In these cases, Ionic alters the “standard” execution path, however it is defined, in a way that was not intended or contemplated by the original developer.

devices to prevent such unlogged communications and help companies comply with their regulatory obligations. However, such products modify the standard execution path of software while the user is visiting controlled sites in order to allow for externally provided instructions. Specifically, Ionic provides an installer to introduce the Ionic software, and the Ionic.com platform communicates with the Ionic software to deliver policy rules for each site. As such, they, too, appear to be covered under the proposed rule.

Each of these products appears to come squarely within the scope of the controls, even though they are purely defensive and protective in nature. Even if they are classified as “intrusion software,” which is not itself directly controlled, as a practical matter they cannot be used without equipment and software that operates, delivers, and communicates with them, or developed without the “technology” used to develop them.

The proposed rule would not only capture Ionic’s products. It could capture many add-ons for software that do not come with a plug-in architecture or functionality, because add-ons work by modifying the standard execution path of the software to provide for externally provided instructions in ways the original designer did not intend.¹⁹ For example, the Microsoft Detours library is a key industry tool for software innovation, performance monitoring, and security patching. It is designed to generate “hooks” that intercept and modify the standard execution path of a target program and then generate instructions to deliver these execution changes into the program. It also captures a variety of tools that extract or modify data for legitimate reasons. For example, remote management software allows system administrators and information technology (“IT”) help desks to control computers remotely and often to extract information, such as to collect activity reports, from these computers to resolve any issues.

c) May encompass all software innovation

The broad and undefined phrase “modifying a standard execution path of a program or process” has the potential to encompass all software innovation. Such innovation often involves building on other people’s software, including defeating the protective countermeasures of the original developer or the system their software is running on, modifying the standard execution path that the original author wrote, and experimenting with how the software runs. As such, “modification of the standard execution path of a program or process in order to allow for externally provided instructions” could include many legitimate and innovative software engineering practices.

The proposed language similarly would appear to capture all third-party software developers—i.e. developers creating software to integrate with other companies’ products.

¹⁹ As discussed in footnotes 17 and 18 it is ambiguous whether the proposed language would also capture the numerous add-ons for browsers and other programs which do have an add-on architecture (i.e. add-ons that *were intended by the original software designer*). Such add-ons could be considered to alter a “standard” or “default” execution path, even though the original author intended the modifications to be made. This ambiguity highlights the importance of defining “modification of the standard execution path of a program or process.”

These developers create software to cure a flaw in or add new functionality to an existing program, which the existing program's authors did not originally intend. To add this functionality seamlessly, the new program by necessity takes steps that intrude on the old program, defeat any relevant countermeasures, and implement the new program's instructions to modify the "standard execution path." For example, performance monitoring tools are used by developers to improve their software and by system owners to understand why their systems are running slowly. They work by hooking into the system in different places to time how long certain processes take. To do this, they must defeat the system's protective measures to inject the hook, and then modify the standard execution path of the program in order to record the times for each process. Similarly, automation tools are used to automate the actions of a system user in order to test that a system is working properly. Such tools, when working with older programs that did not intend such automation, must inject hooks (in a way that defeats protective countermeasures) to change the standard execution path to allow simulation of the user's actions. This process is simply how new functionality is developed and added.

C. Exceptions to the Definition of Intrusion Software

The proposed rule's explicit exceptions to the definition of "intrusion software"—such as hypervisors, debuggers, software reverse engineering ("SRE") tools, and digital rights management ("DRM") tools²⁰—are inadequate and ambiguous. As an initial matter, considering the items described above, these exceptions are insufficient even for existing tools; and this approach (simply adding exceptions for legitimate products) is altogether ineffective because even if each and every legitimate product currently available was listed, it is not possible to predict which tools may be invented in the future.

Additionally, it is not entirely clear how these exceptions apply to products that can be used for both an "excepted" purpose (like DRM), but also have malicious uses. For example:

- Packers: These tools take "intrusion software" and put them into a format that is compressed using a unique algorithm, protected, and delivered to a target. If such a file contains malware, it will avoid setting off an antivirus product's alert unless that antivirus software knows its algorithm or runs it in a "sandbox" type environment. Such a tool, used in this way, seems to be the type of product BIS is trying to control—it delivers exploits. However, the same tools are also used in legitimate activities, such as for DRM purposes. In that context, the "packer" similarly takes information and compresses it into a format that is more difficult to analyze, but it does so in order to protect data from unauthorized access. Although this DRM purpose is explicitly excluded under the current proposed rule, it is unclear how BIS intends to differentiate between such products—they are technically indistinguishable, with only a different end-use. Again, the controls come down to intent.
- Obfuscators: These products are used to protect intellectual property by protecting its code from analysis. However, malware can also be run through such a tool to protect its code from analysis (making it harder for defenders to understand how it works and defeat

²⁰ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28858 (May 20, 2015).

it). These products work the same way and are, technically speaking, often the same. However, some are marketed for the protection of intellectual property and for other legitimate uses; while others are marketed for the protection of malware. It is, again, difficult to see how BIS intends to differentiate between such products or determine when they are designed for intrusion software versus other legitimate uses.

Under the proposed rule, it is not clear how BIS intends to handle these types of products, which may have both “excepted” uses and malicious uses. It seems difficult, if not impossible, to distinguish between them at a technical level; and if BIS intends to use an intent-based approach, it should do so explicitly.

D. Controlled Items Related to “Intrusion Software”

1. Systems, Equipment, Components, and Software (ECCNs 4A005 and 4D004)²¹

The proposed ECCNs 4A005 and 4D004—for systems, equipment, and components, as well as software, that is “specially designed” or modified for the generation, operation or delivery of, or communication with, “intrusion software”—are too broad to be workable. As discussed above in Section II.A, the proposed controls effectively capture any “intrusion software,” including legitimate security tools, because these tools cannot be used without generating, operating, delivering or communicating with them. Even beyond that, as BIS has recognized, the language of the ECCNs themselves catch some legitimate defensive tools, such as for penetration testing, because they are themselves command and delivery platforms for “intrusion software.”²² These ECCNs would catch innumerable other purely defensive products, in addition to penetration testing tools.

a) Network Penetration Testing Products

As recognized by BIS, certain network penetration testing products will be captured by the proposed controls.²³ This result is inevitable because, like so many cybersecurity defensive and testing measures, the only difference between penetration testing and malicious hacking is the intent of the person using the tool. Companies who want to extensively test their systems need to go further than using basic penetration testers, which often only capture common vulnerabilities. These companies hire security professionals to access and test their systems using many of the tools and tactics that an adversary would use. Without using these same tools, there is no way to test that a system is secure against them. In other words, anything that controls the tools will make legitimate security penetration testing much more difficult, and these advanced penetration tests are critical to the security of companies and their products.

²¹ Existing ECCN 4D001.a, as it relates to “intrusion software,” is also of concern to the extent it controls software “specially designed” or modified for the development or production of the products described herein.

²² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015); FAQs #18, #29.

²³ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015); FAQs #18, #29.

For example, Symantec Corporation (“Symantec”) engages in extensive and rigorous internal product penetration testing for every new product that it sells to make sure it is safe for its customers. The testers use various systems (including hardware and software) to conduct the testing, and, during the testing process, write their own code to find vulnerabilities and exploit them. They then write a report containing all of the technical information they obtained in the testing process, including on vulnerabilities and exploits. This report is shared with the necessary people in Symantec, so the remediation to close those vulnerabilities can be swiftly developed and implemented.²⁴ This entire process involves Symantec’s labs both inside and outside the United States, and can also involve third parties who may or may not be in the United States. Most, if not all, major cybersecurity companies and information technology manufacturers use this type of penetration testing to ensure the safety of their products and networks.

This type of penetration testing is a normal security procedure on the customer side in addition to the supplier side. Such extensive testing of IT systems and networks is commonplace in many industries, including the nuclear power industry, electricity generation and distribution, financial services, and health care. Moreover, those customers often only buy software products to put on their networks and systems if the sellers can certify that the products are safe, including having been put through extensive penetration testing. The proposed rule’s controls on such penetration testing products and processes would severely hamper the current processes these industries and their suppliers go through to ensure their systems and products are safe.

b) *Other Tools*

There are various other purely defensive tools that may also be covered by the new ECCNs 4A005 and 4D004.

First, sandboxes for malware analysis. These tools use hypervisors to contain malware, and communicate through hypervisors to observe and communicate with malware. Considering the broad scope of the term “communicate,” these sandboxes, which are designed to communicate with malware in order to analyze it and monitor its processes, are potentially caught. Additionally, these sandboxes must have parts that take the malware they find on systems or networks and “deliver” it into the hypervisor in order for this analysis to occur. While hypervisors themselves are excluded from the definition of “intrusion software,” programs that “deliver” malware to hypervisors, “house” the “intrusion software” and ensure it is isolated, and then “communicate” with it are not so clearly excluded.²⁵ Similar products include:

²⁴ Additionally, if during this process Symantec learns of a vulnerability in someone else’s system, it shares that information with the company involved, which may also happen to be outside the United States.

²⁵ While sandboxes are explicitly included in the definition of “protective measures,” it is not clear whether they would also be (1) “intrusion software” itself, or (2) items under 4A005 or 4D004 that “communicate” with intrusion software. *See* Section II.B.1 (discussing how monitoring tools and protective countermeasures can also be intrusion software and expressing uncertainty as to whether the proposed controls would apply to such products).

- FireEye’s detonation chamber technology. This technology is present in many FireEye, Inc. (“FireEye”) products and allows users to execute suspicious email attachments, binaries and web objects, mobile applications and malware that may be resident in file content and malware stores against a range of browsers, plug-ins, applications, and operating environments that track vulnerability exploitation, memory corruption, and other malicious actions in a secure virtual environment. If an attack is identified, FireEye technology captures call back channels, dynamically creates blocking rules to protect the malicious code from infecting the system and transmits this information back to the FireEye network. In order to accomplish this, FireEye technology must communicate with intrusion software, extract data from a computer or network-capable device and modify the standard execution path of a program or process. This behavior seemingly falls squarely within the plain language of the proposed ECCNs.
- Emulators and other virtualization projects. These products re-implement the services that a computer provides (i.e. a symbolic execution) in order to emulate a program. They then capture malware, let the malware interact with the emulator, and monitor all instructions executed. They are important tools for defensive analysts to understand malware, especially as malware attacks on companies rise. Companies that provide such full system emulation approaches include LastLine²⁶ and BlueCoat.²⁷ Such items are necessary not just to run the malware, but to communicate with it and observe it to help security professionals obtain a deeper understanding of it and its threat indicators.²⁸ This communication with malware, even though it is for purely defensive purposes, would again appear to be covered by 4A005 and 4D004.
- Honey pots. “Honey pots” are “fake” computers that are purposely set up as virtual machines or simply software pretending to be a computer. The goal is to have malware infect these “computers” so defenders can observe it. However, once these “honey pots” become infected, they must communicate with the malware, and allow the malware to communicate back. Under the language of the proposed ECCNs, these purely defensive products appear to be covered and controlled.

Second, this language could capture rescue tools for systems that have already been compromised by malware. These recovery tools are used to regain control of an infected system after it has been infected by malware—for example, a “cryptolocker,” which encrypts all of the users’ files for a ransom. As discussed above in Section II.B.2.a, these rescue tools could themselves be classified as “intrusion software”; but even more simply, because they must

²⁶ Lastline Data Breach Platform, Lastline, <https://www.lastline.com/platform/security-breach-detection>.

²⁷ Malware Analysis Appliance, Blue Coat, <https://www.bluecoat.com/products/malware-analysis-appliance>.

²⁸ These products raise the question of whether “communicate” with malware means just pushing and pulling data back and forth (for attackers, this means command and control data, which sends instructions on what to do and the exfiltration of data from systems without the user’s or administrator’s knowledge), or whether it also includes hooking into malware and/or the system it runs in to monitor and analyze its execution.

“communicate” with the malware in various ways (including altering its execution path to interrupt it and regain control of the system, as well as extract data from it, such as the encryption keys to recover the stolen files), these tools appear to fall directly under proposed ECCNs 4A005 and 4D004.

Third, Automated Exploit Generation (“AEG”) tools automate the process of finding vulnerabilities by generating exploits.²⁹ These products can be used for offensive, as well as purely defensive, purposes. AEG is critical to defensive efforts because of the innumerable vulnerabilities in software. Companies must be able to quickly and efficiently determine which of these vulnerabilities are actually a threat (including some way to rank them). For example, if a vulnerability cannot be weaponized (i.e. standard protective measures are able to defeat it), it is not as big of a concern. AEG tools seek to generate “intrusion software” to test which vulnerabilities are of high or low severity. This process allows researchers to pinpoint for vendors the most dangerous threats and provide them with the deeper understanding of these vulnerabilities that is necessary for them to create a true defense. If such products are controlled, as they appear to be under the proposed ECCNs (because their entire purpose is to generate exploits), the rule would control the tools and research that is the most relevant and valuable to companies trying to protect themselves.

Additionally, encoders are tools that can be used to deliver “intrusion software” to a system, but also have legitimate uses not related to “intrusion software.” Such encoders can be used by malicious actors to deliver “intrusion software” because they take shell code, and put it in a format that can be delivered to a target without interference from protective countermeasures by masking any characters that would have been denied by such measures. However, the same class of tools, such as Base64 encoders, are also commonly used in emails and attachments to ensure that binary data is kept intact when stored and transferred over media that is designed to deal with textual data.

Finally, Return Oriented Programming Compilers (“ROPC”) help generate software that can be used in an exploit technique called Return Oriented Programming (“ROP”) to help test defenses against these ROP exploit techniques. This is not the standard way of generating code, and so could be considered to be designed to generate these ROP exploit codes. Such compilers generate ROP code, which overcomes data execution prevention (“DEP”) and may therefore be seen as designed to defeat protective measures. Thus, these compilers could be considered designed for the generation of “intrusion software,” even when used for defensive testing or research purposes.

2. Technology required for the development of intrusion software (ECCN 4E001.c)

The proposed rule adds new ECCN 4E001.c for technology required for the development of intrusion software. This control is very broad, with far-reaching consequences for the cybersecurity community, which depends on rapid and detailed information sharing across the

²⁹ For example, ForAllSecure, Inc. is a start-up company that provides automatic software to test for bugs in programs, including determining the bugs’ exploitability and prioritizing the bugs by their exploitability. *See generally*, ForAllSecure, Inc., *Mayhem: Software Testing Made Easy*, <http://forallsecure.com/mayhem.html>.

globe. As an initial matter, this proposed ECCN would control any technology for the development of cybersecurity tools that may be classified as “intrusion software,” such as those discussed above in Section II.B. But discourse, innovation, and experimentation are critical to developing new cybersecurity tools. These controls would severely damage global cybersecurity companies’ (such as Symantec’s and FireEye’s) ability to engage with their research and development teams abroad, which often closely collaborate with their U.S. teams in developing their cybersecurity products.

This proposed ECCN would severely restrict cybersecurity research and defense more broadly, including research and reporting of vulnerabilities and threat intelligence sharing. These effects seem to be recognized to some degree by BIS already, as the preamble to the proposed rule states that the technology that is proposed to be controlled includes “proprietary research on the vulnerabilities and exploitation of computers and network-capable devices.”³⁰ But BIS does not appear to have recognized the effect these controls on such “proprietary research” would have on global security companies.

While this section focuses on ECCN 4E001.c, the same concerns apply to 4E001.a, “technology” for the “development,” “production,” or “use” of equipment or software controlled by 4A or 4D. ECCN 4E001.a would inevitably control technology (including technical discussions) for the development, production, and use of the purely defensive items that interact with “intrusion software,” such as those discussed above in Section II.D.1.

a) *Vulnerability Assessments and Testing*

Security vendor research groups and security companies, such as FireEye, work with “proprietary research” on vulnerabilities and exploitation every day in their labs across the globe when they conduct vulnerability assessments and testing. In fact, FireEye has a zero-day focus group that conducts this type of proprietary research and reports its results to vendors on a regular basis. When these companies find vulnerabilities, they need to report them and develop a defense as soon as possible. To do so, they need to share not only the vulnerability and exploit, but the information on how the exploits work, including the technology to develop them. To secure systems, defenses need to be developed within days of identifying vulnerabilities, staying as close to real-time as possible; such security gaps cannot wait weeks or months for a fix. The customer expectation is “as fast as possible” and the company that is faster at creating and sharing fixes and other intelligence has the competitive advantage. In the past year, FireEye has itself seen that entire cycle (from finding a vulnerability, understanding its exploitability, developing a patch and deploying it) take as little as 24 hours. But they are global companies and not all of their researchers are in the United States; this work is not even always completely internal to the companies. For example, many U.S. cybersecurity companies have official and unofficial sharing agreements, including for information regarding malware, all over the world

³⁰ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28854; see also FAQs #10 and #19 (recognizing associated “technology” that is controlled may be transferred with the reporting of a vulnerability and exploit); see also FAQs #24 and #25.

with security groups such as other countries' Community Emergency Response Teams ("CERTs").

Cutting U.S. companies off from interacting with these international groups will result in a dramatic decrease in the scope of U.S. security companies' (like FireEye's) knowledge into the global threat landscape, reducing their understanding of which types of malware are being used by malicious actors. Without this type of broad and up-to-date knowledge (and in this industry, knowledge needs to be updated on a daily or even hourly basis), U.S. companies' ability to contribute to the collective defense and protect their customers, including major U.S. companies, the U.S. government, and entities connected to U.S. critical infrastructure, would be greatly damaged. Particularly considering the policy of "presumptive denial" for items that incorporate "zero-days," this proposed rule could cause large numbers of zero-days that companies such as FireEye report responsibly to security vendors every year to go unreported because such reports necessarily include controlled information such as how the exploits work and the technology used to develop them. But it would do little to stop their continued use by malicious actors. The result would be a serious loss for the security community as a whole. And the foreign partners of these companies may also stop providing similar information to U.S. companies.

Similarly, though providing vulnerability testing services through a different model, companies like Synack, Inc. ("Synack"), who work with a talented global community of independent researchers, will also be severely affected by these controls on "technology." Synack recruits a network of researchers that spans thirty-six countries and combines their knowledge and expertise to conduct extensive vulnerability assessments for its customers, often global companies whose systems also span internationally. Through Synack's secure platform hosted in the United States, these researchers access its customers' systems. They find and analyze vulnerabilities, including by writing code to develop exploits to test the vulnerabilities' exploitability; then, they provide Synack with a vulnerability report that includes information on the vulnerability, how it was discovered, and how it was exploited, as well as information regarding their assessment of the severity and impact of the vulnerability on the customer's business. This information often incorporates information on "zero-days," since most of the vulnerabilities are previously unknown and do not yet have a fix. Synack's operations team validates the information and provides it to its customers. Each step in this process may involve foreign nationals—including the researchers, the Synack operations team, and the customers—either within or outside of the United States. The information that is shared inevitably includes in-depth technical information for the development of intrusion software (including how the vulnerabilities are exploitable and how the exploits work). This process would be inconceivable if Synack was required to obtain a license to communicate about each vulnerability report it receives or shares with its researchers and customers in various countries, especially considering that the company could potential face presumptive denials where such reports involve information on zero-day exploit capabilities.

b) *The difficulties in determining the scope of the "technology" will inevitably chill discourse among researchers.*

It is not clear how technical or specific a discussion would have to be before it would be considered controlled "technology," a level of uncertainty that would be sure to chill important

activity in this area. The definition of “technology” would encompass discussions between researchers about vulnerabilities and the means of exploiting them if they are sufficiently technical (i.e. they allow for the operation or building of intrusion software or a related item that is controlled). But these are discussions that inevitably occur both in the process of reporting a vulnerability and in developing a defense for it, as well as developing and innovating cybersecurity tools more generally.

BIS’s attempts so far to clarify the scope of the technology controls are not encouraging. In FAQ #4, BIS attempts to clarify what types of information would be and would not be controlled as technology for the development of intrusion software; however, the examples seem inconsistent with the definition of “intrusion software” and related controls. For example, BIS states in FAQ #4 that fuzzing, “trying different inputs,” and analyzing execution, including decompiling and/or disassembling code and duping memory, are not covered. However, these are common ways to generate zero-day exploits. It is unclear why BIS would state that these techniques for developing exploits, which would likely be controlled under ECCN 4D004, would not qualify as controlled development technology. “Fuzzing” provides invalid, unexpected, or random data to the inputs of a computer and then monitors the computer for crashes. The crashes caused by the “fuzzing” are then analyzed to determine if they involve a vulnerability that is exploitable. That is the purpose of fuzzing—to provide the information that is “required for” the development of the exploit. The first one to determine if such a crash is in fact exploitable, by reaching and exploiting it, discovers and generates a “zero-day” vulnerability.³¹ Without this full analysis, the vendor cannot know whether a crash has been caused by a non-exploitable bug or represents a true security vulnerability. BIS muddies the picture about which forms of technology are controlled by stating without any apparent reason that these particular methods (and the resulting information), which would appear to fall squarely within ECCN 4E001, are not controlled.

The difficulties in determining what is included under the proposed technology controls³² will have a disproportionate impact on the many small companies and independent researchers

³¹ Microsoft’s !exploitable (pronounced “bang exploitable”) is an example of such a program. This product is a Windows debugging extension that provides automated crash analysis and security risk assessment. It works by first determining the uniqueness of a crash and then assigns an exploitability rating for the crash.

³² In FAQ #4, BIS states that the only technology that would be controlled is that which is “required for” and peculiarly responsible for achieving or exceeding the relevant characteristics of controlled items related to “intrusion software.” But “peculiarly responsible” is difficult to interpret and apply. First of all, that concept is not currently defined in the EAR, although it is used in the definitions of “specially designed” and “required.” Its use in the definition of “specially designed” makes it integral to the definition of “intrusion software,” and the fact that it is part of the definition of “required” means it must be considered in any evaluation of the applicability of technology controls. Even without the ambiguities around the meaning of “peculiarly responsible,” the “specially designed” analysis is quite complicated. BIS has set out a definition for “peculiarly responsible” in the proposed rule that was published on June 3, 2015 that may provide some clarity. *See Revisions to Definition in the Export Administration Regulations*, 80 Fed. Reg. 31505, 31517 (June 3, 2015). But until that rule takes effect this term

who are not as well versed in export controls and who may be shut out of the market, or forced underground, because they do not have the resources to be able to comply with these complex and ambiguous rules. These rules were developed for major industrial and defense companies and do not work well in a market whose foundation is independent researchers and small companies with little overhead.

These ambiguities create an extraordinary grey area with the potential to chill innovation and discourse. If researchers are prevented or discouraged from engaging in covered communications, even within their own companies, the reporting of vulnerabilities and the ability to produce defenses effectively and quickly may be significantly affected.³³

E. Controlled “Surveillance” Items (ECCN 5A001.j)

The proposed rule adds ECCN 5A001.j for IP network communications surveillance systems, equipment, and components.³⁴ While this ECCN involves many elements that work to limit its applicability, concerns still exist with its language, which, similar to the “intrusion software” items, lacks a distinction between defensive and offensive items and could include tools companies use on their own networks to monitor activity and find hackers, as these tools look closely at the data that is moving through the companies’ networks in order to help keep it secure.

1. ECCN 5A001.j could capture tools used to help keep networks secure

For example, this definition could capture any of FireEye’s network appliances (such as FireEye endpoint and network forensic and investigative tools) because these products intercept network traffic, reassemble it, inspect and analyze it, and block or modify it when necessary. While likely not being the type of system that BIS intended to capture, these products come very close to the definition in ECCN 5A001.j as it currently stands, and, as demonstrated below, will only continue to resemble it more with time.

For example, network security monitoring tools, such as those available from FireEye, meet all of the elements in 5A001.j.1: they conduct analysis at the application layer, extract selected metadata and application content (including attachments, etc.), and index the extracted

remains undefined. In any event, the scope of BIS’s technology controls will remain beyond the capacity of many small companies and independent actors in this industry to analyze and comply with.

³³ Context is particularly important here. Many independent researchers are only now getting comfortable with responsibly reporting vulnerabilities to companies without the fear that the company will take legal action against them for accessing their systems. Enacting regulations with the types of ambiguities in this proposed rule would unnecessarily create fear of export enforcement action from the government for such reporting, and consequently reverse this critical progress.

³⁴ Relatedly, existing ECCNs 5D001 and 5E001 will control the software and technology related to these IP network surveillance systems. As discussed above, the breadth of these controls, particularly those around “technology,” are particularly concerning in the cybersecurity realm where detailed communication and collaboration is essential.

data (to inspect it, and modify or block it when necessary). They also have “hard selectors” passing through their system, such as email address and recipient information when processing email. Additionally, they meet element 5A001.j.2.a because they use email addresses, such as when an email address is known to be used by a bad actor (e.g. in a spam campaign), as “selectors” to be searched and targeted so an alert is triggered when emails from that address pass through the network. Finally, as to 5A001.j.2.b, their ability to “map relational networks” is only increasing. Such capability is desirable in a security monitoring system because it enables the system to correlate information and track two important groups: (1) the group of people being targeted or affected by the malware or attack, and (2) the group of attackers.

Similarly, this ECCN could cover email malware virtualization tools that help to secure and protect email, such as FireEye’s Email Security (EX Series). Such tools extract content from emails, including determining whether there are .zip file attachments and, if needed, look through human readable content to extract passwords for such files. They may also extract .pdf attachments, which are often used by malicious actors to deliver exploits to unsuspecting targets. These tools monitor email and extract human content to scan for malware and quarantine it before it can affect the target system. Such security tools, if of a “carrier class,” could come within the definition of IP network communications surveillance systems despite being completely defensive.³⁵

2. “Carrier Class” is not sufficiently defined.

Additionally, the proposed rule does not define “carrier class” to the degree necessary to enable companies to determine if their products are covered. BIS has attempted to narrow the scope of ECCN 5A001.j in its FAQ #14 to clarify that “carrier class IP network” was meant to capture systems at a national level IP backbone, such as those that handle data from an entire city or country. However, BIS also states that “carrier class IP network” was not defined because it was difficult to put precise parameters on the concept. Thus, no definable metrics (such as gigabytes per second, which is often used to measure network size) are associated with this “carrier class” parameter.³⁶ There are many different sized “cities” and “countries” and this

³⁵ Depending on how broadly the rule is interpreted, it could even cover items used by many companies, including Symantec and its customers, to make sure that their products (which are sold and downloadable online) are not sold to individuals from sanctioned countries. These items track and block IP addresses, so that individuals from these sanctioned countries cannot purchase online products. To do so, they monitor the network for IP addresses from sanctioned countries, pull out these IPs, and act on this information by blocking these users’ access to their website. These tools place tracking script on the companies’ websites in order to extract data and track the movement of users throughout the websites, and then feed this information into a system which can be searched for selectors, such as IP addresses. These tools are ubiquitous throughout the industry and are the only way to ensure that individuals from these sanctioned countries do not access online products. If there is any ambiguity whether these products would be covered, it could necessitate licenses for thousands of products.

³⁶ Even if BIS did put a certain “bandwidth” number on the scale, it would quickly be outdated—five years from now the bandwidth for a city may be commonplace for a house. Similar to how the definition of “supercomputer” fifteen years ago is no longer significantly different from a

metric seems entirely inadequate to help companies determine where their products fall.³⁷ For example, it is entirely possible that the DOD network is itself bigger than most cities' networks.³⁸ Also, there are large universities that are bigger than small cities. Would this mean the tools used to monitor and inspect the traffic in and out of these networks would be covered by this rule? While BIS may have meant to exclude most security monitoring products (including FireEye's products discussed above) with the "carrier class" limitation, this scale needs to be more clearly defined. If BIS cannot itself determine a clear place to draw the line, it is difficult to see how it can expect companies to be able to determine if their products are covered.

Additionally, it is unclear how the line would be drawn for "components" for "carrier class" IP network communications surveillance systems. Often the difference between a "carrier class" network surveillance system and a smaller system is not a technical difference—the same components can be used for each. Often, more components (more computers, etc.) are used to bring the surveillance system from a small neighborhood to the level of a larger region. A "load balancer" is then used to spread the work among the different appliances—each "component" handles a certain amount of traffic, which is multiplied by the number of components to get the larger scale (this is called "horizontal scaling" and is core to the engineering systems for modern traffic rates). It is thus unclear whether components for "carrier class" IP network surveillance systems would include any components that can be used in such a larger system (which would seemingly then encompass all smaller systems using the same components).

F. Specially Designed

All of the proposed controls are limited by the term "specially designed." But that term of art, defined in Part 772 of the EAR, can be difficult to apply in practice, particularly for smaller companies and independent operators that make up much of the U.S. cybersecurity industry. Moreover, the definition of "specially designed" does not seem to account for the

common desktop, such use of "bandwidth" as a metric, even if it seems ridiculously large today, in the future will not be.

³⁷ For example, North Korea has only 1,024 official Internet protocol addresses, fewer than many city blocks in New York. The United States, by comparison, has billions of addresses. Nicole Perlroth and David E. Sanger, *North Korea Loses Its Link to the Internet*, NY TIMES (Dec. 22, 2014), http://www.nytimes.com/2014/12/23/world/asia/attack-is-suspected-as-north-korean-internet-collapses.html?_r=1. Similarly, some estimates have put the bandwidth of North Korea's nationwide optical network at 2.5 Gbps. See *Asia Internet History*, available at: <https://sites.google.com/site/internethistoryasia/country-region-information/north-korea-korea-democratic-peoples-republic-of>. By comparison, Comcast has begun offering 2 Gbps fiber-to-home service in some areas; and already offers 10 Gbps fiber service to businesses. See Jon Brodtkin, *Comcast doubles Google Fiber with 2 Gbps symmetrical fiber service*, ARS TECHNICA (Apr. 2, 2015), available at: <http://arstechnica.com/information-technology/2015/04/comcast-doubles-google-fiber-with-2gbps-symmetrical-fiber-service/>.

³⁸ See, e.g., *JIE: How DOD is building a bigger network that's also a smaller target*, DEFENSESYSTEMS (Feb. 23, 2015), <http://defensesystems.com/Articles/2015/02/23/Joint-Information-Environment-JRSS-security.aspx?Page=4> (describing upgrades to the DOD network backbone that will increase the bandwidth to 100 Gbps).

realities of the information technology industry. For example, one key reason for finding that an item is not “specially designed” is that it was developed as general purpose, i.e. without knowledge that it would be used in or with a particular commodity or type of commodity.³⁹ But the note to that release paragraph says that in order for it to apply, there must be contemporaneous development documents that, in their totality, establish the necessary elements; absent such documents, the commodity may not be excluded from being treated as “specially designed.”

This provision does not account for the realities of the technology industry for several reasons. First, there often are no “documents” or any records at all showing the intent of a developer. Software developers often work alone and independently of any organization, so there would be no reason for them to document their design intent. Second, developers often experiment in a variety of ways, not always knowing exactly what they will uncover or create. In other words, they often do not set out on a particular mission that can be retrospectively traced to determine what their intent was in developing a particular product. That absence of a development intent trail would make it impossible to invoke this important exception to the “specially designed” concept for items that can be used for multiple purposes, such as the packers and obfuscators, discussed above in Section II.C. This is just one small example of how the existing structure of the EAR was not made to accommodate controls on such a unique, dynamic and complex industry. Attempting to squeeze a square peg into a round hole in this instance would have profoundly negative consequences.

G. “Publicly Available” and Intent to Publish

The EAR contain carve-outs for items that are “publicly available” or intended to be published. In its FAQ #5 on intrusion and surveillance items, BIS explains that the EAR does not control the export of data to conference organizers with the intent that it will be published at a conference. See also FAQ #6, which states in response to the question whether the regulations will make it more difficult to alert the world of exploitable bugs, that there are no restraints on publishing information otherwise subject to control. While it is generally positive to spell out clear exceptions in such a way, this particular provision raises serious concerns for the cybersecurity industry, because zero-day exploits and their associated technology often are not made publicly available until there is a defense available and released. The “responsible disclosure” process is as follows: a vulnerability is found, reported to the system or software vendor and discussed to determine impact and priority, then a defense may be developed and delivered to the vulnerable system, and after that a company may decide to publish the vulnerability. Companies often do not want a vulnerability or exploit to be published before a defense is released. For critical infrastructure systems in particular, for which the timeline for patching vulnerabilities is very slow, taking as long as twenty years in some cases, encouraging the publication of exploits before a fix is available may be unacceptably dangerous.⁴⁰

³⁹ Paragraph (b)(5) of the definition of “specially designed.”

⁴⁰ See, e.g., Kelly Jackson Higgins, *The SCADA Patch Problem*, INFORMATIONWEEK, DARKREADING (Jan. 15, 2013), available at: <http://www.darkreading.com/vulnerabilities---threats/the-scada-patch-problem/d/d-id/1138979?> (noting that only about 10-20% of utilities and other organizations running industrial control systems install patches that vendors release,

On the other hand, failure to allow the prompt exchange of technology and information related to the vulnerability would also be dangerous, as it would stall the process for developing a fix. In this way, the proposed rule constitutes a threat from both sides to the cybersecurity industry. It is not clear whether there is an acceptable solution within the confines of the EAR as they stand today, but it is clear that trying to fit this dynamic industry into the pre-set mold of outdated export control regulations will present real complexities that need to be examined closely before any final regulatory action.

Furthermore, many cybersecurity conferences may fall into a grey area in the rules. Typically these conferences include many nationalities but portions of the event may not qualify for the carve-outs that apply to those that are “open” or “public.” For example, the primary revenue stream for many such conferences involves private training offered by the speakers (either before or after the conference) that goes into more technical detail than could be covered during the conference. Additionally, some sessions may not allow all technically qualified individuals to attend, for instance by excluding members of the press or government.⁴¹ Because they may not qualify for the relevant carve-outs, in order to avoid the constraints imposed by the proposed rule, such conferences would in all likelihood be offered outside the United States in the future in order to facilitate attendance by foreign researchers, students and professionals. This would be just another way in which the center of gravity for this critical industry may move offshore, with potentially serious long-term consequences for U.S. national security.

III. LICENSING POLICIES

Due to the broad and ambiguous controls discussed above, the strict licensing regime proposed by BIS for cybersecurity items is alarming. The following sections discuss the Coalition’s key concerns regarding the proposed rule’s licensing policy, the effects of including deemed exports and intracompany transfers within this strict regime, and the burden of the proposed licensing application process on a cybersecurity industry that is constantly evolving and dependent on rapid sharing of information.

A. Strict Requirement for Licenses to All Destinations, Except Canada

The requirement for licenses to all destinations except Canada for cybersecurity items is unduly restrictive.⁴² Adding to the concern is the ineligibility of controlled items for any license exceptions, except certain provisions of License Exception GOV (exports to or on behalf of the U.S. government).⁴³ The rule also explicitly removes cybersecurity items’ eligibility for License Exceptions ENC, STA, and TSR. These unusually strict proposed licensing policies do not take

because of the complexity involved in avoiding system interruptions during the installation process).

⁴¹ Cf. 15 C.F.R. § 734.7 (information is “published” when it is released at an “open conference,” which means that, among other factors, all technically qualified members of the public are eligible to attend).

⁴² See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28857-58 (to be codified at 15 C.F.R. § 742.6).

⁴³ *Id.* at 28856-57 (to be codified at 15 C.F.R. § 740.2(a)(19)).

into account the realities of the cybersecurity industry and are more stringent than the existing licensing policies for virtually all other items controlled under the EAR. The very existence of a licensing requirement in this industry would hinder U.S. cybersecurity activity and forestall the development of new capabilities.

The reality of the cybersecurity business is that vulnerabilities would be exploited by malicious actors while defensive products would become obsolete waiting for licensing approval. In the penetration testing context, BIS licensing would be completely unworkable. Penetration testers do not know what vulnerabilities they will find when they begin the testing; they follow any leads they discover and write code as they go to develop the exploits to test the vulnerabilities they find. And when penetration testers find something, they cannot just share the proof-of-concept exploit with the company that hired them (or in some cases the company did not hire them—they are freelancers). They need to share their in-depth technical knowledge on (a) the root cause of the vulnerability, (b) how they found it and generated an exploit against it, (c) their estimations of the ease of exploitation by malicious actors, and (d) proposed solutions to the problem, which (as the penetration testers did not develop the system being tested) requires in-depth technical discussions between the penetration testers and the company's engineering teams to suggest a workable solution (or 'patch').⁴⁴ It would be seemingly impossible to write a license application for such a project before it began, as the necessary information would not be known.

Furthermore, when a company engages in penetration testing it involves finding a company's most sensitive exploitable vulnerabilities (in order to develop patches for them). For this reason, the testing often takes place in a secure and isolated environment (a "black box"), with the information on the vulnerabilities and exploits protected while in the black box, and destroyed once the testing and patching is completed. If this information were to be leaked or otherwise released, the effects on the tested company and its customers could be crippling. If U.S. security companies that provide such testing services could be required to put this information into a license application, their customers would choose to use non-U.S. providers so to avoid what they may see as an unnecessary danger. For many companies, including Symantec, this penetration testing process involves collaboration with individuals outside the United States as well as foreign national employees within the United States, both of which would require licenses under the proposed rule. For example, Symantec's internal penetration testing process involves sharing information with its labs in Europe and India and also often involves third parties whom Symantec hires to test its systems. Also, if and when a company does face an actual breach of its systems, U.S. security companies have "incident response" teams, who are ready to go at a moment's notice and sometimes have to deploy within 24 hours when a problem is discovered—these teams do not have time to get a license.

Additionally, the international cybersecurity community includes a significant number of independent researchers, many of whom have only informal relationships with U.S. cybersecurity companies. Many independent researchers are completely unaffiliated with any

⁴⁴ See also *supra*, Sections II.A and II.D.2.a (discussing the in-depth back-and-forth dialogue between independent researchers, security companies, and their customers during the processes for vulnerability testing and assessments).

security companies and can appear out of the blue when they choose to responsibly report vulnerabilities. Once a vulnerability is reported, however, companies need to engage in a back-and-forth dialogue with the researcher that would involve technology transfers to understand the vulnerability and its exploitability, and to develop a patch. These vulnerabilities (which if they are new and novel are by many definitions “zero-days”) need to be patched immediately. The entire cycle from finding the vulnerability, understanding its exploitability, developing a patch and deploying it can occur within 24 hours—there is no time to get a license. And even those independent researchers, who act as consultants and experts for companies who are trying to test their defenses and develop patches, often never sign a formal contract or arrangement. These independent actors, who are undoubtedly unfamiliar with the U.S. licensing process and may be reluctant to share their information with the U.S. government, will be discouraged from cooperating with U.S. cybersecurity companies and may choose to altogether withdraw from these informal engagements with U.S. companies if such licensing is required.

Even independent of the problems with applying a strict licensing scheme to the unique cybersecurity industry, the specific requirements for license applications for cybersecurity items would themselves be unduly burdensome. They incorporate the current reporting and registration requirements for encryption products, while eliminating eligibility for the encryption license exceptions. The proposed rule also adds new requirements specific to cybersecurity items that are very burdensome. For example, it would be difficult, if not impossible, for companies to explain how rootkit or zero-day exploit functionality would be precluded from the item. As described below in Section III.B.2, trying to identify how an item supports or precludes rootkit or zero-day exploit capabilities in the first place would be difficult and confusing both because they are undefined jargon terms and because they are often capabilities present in defensive products and research. In addition, determining the amount and type of information necessary to describe the “cybersecurity functions” would also be challenging. The requirement to share source code upon request could hamper the communications and collaboration that are key to building successful defenses by discouraging cooperation with independent software engineers. Those individuals would not stop working, but they would stop working with U.S. companies.

The number of license applications under this rule, for each new product, customer, foreign national employee and business partner, would not only tax the resources of the companies, but would swamp BIS as well.⁴⁵ For example, Symantec estimates that under the proposed rule (in addition to the hundreds of deemed export licenses it would need) it would need several hundred hardware, software, and technology licenses for its products, as well as a couple of dozen of site licenses. Licenses would be required not only for cybersecurity

⁴⁵ It is difficult to estimate the number of cybersecurity companies in the United States that would be affected by this proposed rule, but it is likely in the thousands. Due to the low overhead in this industry, businesses can often be started without external help or capital, making venture capital firms unnecessary. In any event, it is clear that it is an industry that is growing rapidly. *See* Rick Gordon, *The Cyber Security Market Is Hot! Here’s Why*, INFORMATIONWEEK, DARKREADING (May 8, 2014), <http://www.darkreading.com/risk/the-cyber-security-market-is-hot!-heres-why/a/d-id/1251128> (“A dozen years ago the \$3.5 billion security market was dominated by five vendors. Last year, VCs bankrolled 230 startups.”).

companies and researchers but also for their customers. These customers often have individuals (such as in their IT departments), who may be foreign nationals or located in foreign offices and coordinate with the cybersecurity companies to conduct penetration testing or use other defensive tools that may be covered by the proposed rule. The range of companies requiring licenses could include financial institutions, pharmaceutical companies, and other companies in highly regulated areas that must use penetration testing and other covered security products.⁴⁶ And the range and number of companies that choose to (or are legally required to) conduct such testing is growing. In short, requiring companies to obtain licenses for the export of these types of systems, software, and technology would be devastating to the U.S. cybersecurity industry, and—just as importantly—would be a blow to cybersecurity itself.

B. Explicit Licensing Policies for Certain Items

If licenses are required, the licensing policy framework as currently envisioned is at odds with efforts by U.S. companies to implement strong cybersecurity mechanisms. While the proposed rule does state a favorable licensing policy for some items, and a presumptive denial for others, these policies are nowhere near sufficient to assuage concerns and in some instances seem to make little sense. And, outside of these explicit policies BIS has given companies little guidance on what to expect from the licensing process, instead proposing a case-by-case licensing policy to determine if a transaction would be contrary to U.S. national security or foreign policy interests.

1. Favorable Licensing Policy

BIS's favorable licensing policy is not nearly sufficient. It is limited to certain countries based on type of end user: (1) U.S. companies or subsidiaries, but only those located outside Country Group D:1 (includes countries like China, Russia, and Vietnam) or E:1 (Cuba, Iran, North Korea, Sudan, and Syria); (2) "commercial partners" in Country Group A:5 (includes many European countries, plus Australia, Japan, South Korea and Argentina, among others); and (3) government end users in Australia, Canada, New Zealand, and the United Kingdom. There are many important countries that are excluded from this list. For government end users, even most European allies are excluded. And for U.S. companies and subsidiaries, some of the excluded countries are those in which it is most important for U.S. companies to use cybersecurity defenses to ensure their networks are secure, such as China and Russia.

Even if one of these favorable policies does apply, considering the pace at which products are developed and new versions updated (including updates required for continued integration with third party products), companies could be required to repeatedly apply for licenses and would face damaging gaps in their products' ability to integrate with third party products—a result likely to overwhelm both their own resources and those of BIS. And the

⁴⁶ See, e.g., Federal Information Security Management Act (FISMA) of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3544(b)(5); see also *Technical Guide to Information Security Testing and Assessment*, U.S. Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-115 (September 2008); *Penetration Test Guidance*, Federal Risk and Authorization Management Program (FedRAMP), Version 1.0.1 (July 6, 2015). See generally, Section V, below.

complexity, risk and processing time for licenses would chill activity in this industry that operates in real-time. For example, in the vulnerability research context, if a vulnerability is discovered, a company is likely to have teams around the world working on a fix in real time. If the vulnerability is made public, this process becomes a 24/7 race between the defenders and the malicious actors: the malicious actors use the public information about the exploit to develop exploit kits and exploit targets and the defenders rush to develop detections and mitigations and release these updated protections into their products globally. Requiring a license will stall this process for defenders, leading to less secure systems and causing customers to resort to security testing companies that are not subject to U.S. jurisdiction.

2. Policy of Presumptive Denial

The proposed rule includes a policy of presumptive denial for items that have or support “rootkit” or “zero-day” exploit capabilities. This policy is highly troubling in many ways. First, there are no definitions of “rootkit” or “zero-day” exploit capabilities, which are jargon terms that can be interpreted in various ways in different contexts. For example, zero-day exploits could refer to vulnerabilities that no one knows about except the attacker; but, they could also more broadly refer to vulnerabilities for which a patch is not yet available. But more importantly, a policy of denial would be devastating to the cybersecurity industry’s ability to develop and employ defensive products in light of the many critical and legitimate uses that exist for such items.

a) Zero-days

First, the policy of presumptive denial for items with zero-day capabilities would limit the development and delivery of defenses for the most dangerous vulnerabilities, zero-days. Zero-day vulnerabilities and their exploits make up the majority of what is discovered during penetration testing, as these are the previously unknown and unpatched vulnerabilities. In fact, as discussed above in Section II.D.2.a, companies such as FireEye have zero-day focus groups, which specifically research these types of vulnerabilities and must exchange information about their exploitability to develop a defense. If zero-days are defined as vulnerabilities without a released patch, then they are the highest priority items for responsible companies to address, and it would be highly problematic if they were restricted in their ability to get information about such vulnerabilities and associated exploits, technology, and technical details to—and from—their most knowledgeable experts, some of whom will be foreign nationals.⁴⁷ If a company was prevented from closing a vulnerability, the security of its customers would be at risk.

In FAQ #22, BIS explains that the reason for this policy of presumptive denial is that when a rootkit or zero-day capability is incorporated into a product or system, or if an exploit delivery tool is specially programmed to deliver or command this specialized malware, it is

⁴⁷ Relatedly, the patch that these experts develop and need to deploy internationally to close a zero-day vulnerability itself could be considered controlled under the proposed rule. The defensive products that contain the patch have in fact been used in the past by malicious actors to recreate the exploit. Because this ability exists in the very patch that is being exported to close a vulnerability, such a patch could itself be interpreted to be “technology” or “software” to develop or generate a zero-day.

presumed to be offensive by design. The intent appears to be to focus on denying malicious control and delivery platforms. However, that is not the practical effect. In fact, imposing such a harsh licensing policy on the export of tools with zero-day capabilities does not appear to accomplish what it sets out to do. Zero-days are zero-days because of the state of knowledge of others (i.e. they are not publicly known). Thus, this proposed policy would appear to control a delivery tool that carries a zero-day today, even though the exact same delivery tool might not incorporate a zero-day tomorrow (because the exploit has become public). This control makes it very difficult to pinpoint when delivery technology, which itself may stay exactly the same and can be independent of the exploit, is controlled. In other words, the “delivery tools” are often not unique for zero-day exploits; in some cases a generic delivery tool can be used.⁴⁸ The exploit is what is unique, and while the exploit and the delivery tool can be combined into the same tool (i.e. the same set of code), they also can remain distinct (i.e. two distinct sets of code). Delivery tools themselves can remain constant for the same “class” of target vulnerability while being updated with new zero-day exploits. This would appear to create a curious result—zero-day exploits would not themselves be controlled, and delivery tools without zero-days would not be subject to the policy of denial; thus, somebody could theoretically export them separately to be combined overseas, even though if they had been combined earlier any license would have been denied. This framework is clearly unworkable.

b) Rootkits

The presumptive denial for rootkits is similarly confusing. While the functionality of “rootkits” may vary and the term can mean different things in different contexts, a “rootkit” capability is often understood to mean simply that the item can live underneath the user interface and subvert what the user is doing without his or her knowledge. Basically, the rootkit subverts part of the operating system by interrupting it, running “underneath” it, or hooking into it; then, when the operator of the system takes an action, the “rootkit” intercepts that action and modifies or subverts it without the user’s knowledge so that it acts differently than it was intended to.

If this common definition is how BIS interprets “rootkit” capability in the proposed rule (which is unclear since no definition is provided), any software security instrumentation framework could be seen to create a rootkit capability. Security modules often hook into and change the behavior of the operating system. And a fundamental part of most security vendors’ endpoint protection products, including FireEye’s, is its “rootkit” capability. When you install antivirus software, FireEye’s endpoint security products, or various other types of security software, they often work by hooking into the normal operating system, monitoring the data communicated through it, intercepting and inspecting the data, and potentially changing it when it is a threat—all without user knowledge. These “rootkit” capabilities are used in these products

⁴⁸ Additionally, as discussed Section VI.D, the proposed rule is ineffective because it would likely not capture these generic delivery tools, as well as many other common and generic items that have legitimate purposes, but can also be used to deliver, operate, and communicate with malware, including zero-day exploits. See, e.g., Dennis Fisher, *Attackers Exploiting Windows Ole Zero Day Vulnerability*, THREATPOST (Oct. 22, 2014), <https://threatpost.com/attackers-exploiting-windows-ole-zero-day-vulnerability/108958>.

because they are the most effective means of getting into the system to monitor for and catch malicious traffic before it can get into the system.

“Rootkit” capabilities are a common function of legitimate software, not just for cybersecurity. Legitimate programs, such as DRM software, which the proposed rule exempts, could fall under a common understanding of the meaning of “rootkit” capabilities. Other examples include remote control software used by help desk technicians, system administration, technical support, and even anti-cheat mechanisms for video games. None of these programs with “rootkit capabilities” are intended to be malicious, but the proposed rule does not distinguish between those used with a network or system administrator’s or authorized user’s knowledge and authorization and those put there with only the malicious actor’s knowledge. In light of the broad range of legitimate uses for “rootkit” capabilities, a policy of presumptive denial would be inappropriate.

C. Deemed Exports

Applying the deemed export rule under such a strict licensing regime and without any license exceptions⁴⁹ would be devastating to U.S. cybersecurity. Even if BIS was able to craft some kind of blanket licensing authority for major companies, the many foreign nationals who work independently, such as academics and independent researchers, a significant portion of whom have only informal relationships with U.S. cybersecurity companies, would face serious restrictions that would also impact the major companies that rely on their expertise. Furthermore, this would affect companies using cybersecurity products, who would be driven to favor non-U.S. products in order to facilitate access by foreign nationals and overseas facilities.

1. U.S. Cybersecurity Companies’ Employees and Independent Researchers

U.S. cybersecurity companies employ many foreign national researchers, code writers, and others. For example, Symantec alone estimates that under the proposed rule it would be required to get up to 850 deemed export licenses. Given the very high number of foreign nationals employed in the cybersecurity field in the United States, this could mean tens of thousands of employees—or more—could be affected.

That does not even count foreign national independent operators living in the United States, many of whom only have informal relationships with U.S. companies.⁵⁰ Just as with the independent researchers in foreign countries discussed in Section III.A, these researchers often find and choose to responsibly report vulnerabilities to U.S. companies, which then need to engage in a back-and-forth dialogue with the researcher that would involve technology transfers to understand the vulnerability, its exploitability and severity, and to develop a patch. These researchers also act as consultants for U.S. cybersecurity companies when they have particularly useful expertise in a certain vulnerability or type of exploit. But the prospect of having to

⁴⁹ See FAQ #32.

⁵⁰ See, e.g., Acknowledgements, Security TechCenter, Microsoft, <https://technet.microsoft.com/library/security/dn820091.aspx> (listing individuals who disclosed vulnerabilities to Microsoft, including number of individuals who are unaffiliated with any organization and individuals identified only by an alias).

determine the nationality of independent researchers under the sometimes complex nationality rules BIS uses, and obtain the detailed personal information necessary to apply for licenses, is a non-starter. Many independent researchers would disengage from this process altogether at least with respect to U.S. companies, as they would view the drawbacks of this type of regulation as clearly outweighing any benefit they receive from responsible reporting. Such a scenario would be devastating for U.S. cybersecurity.

2. University Research

A large proportion of students and other researchers at U.S. universities in cybersecurity fields are foreign nationals.⁵¹ While publicly available information that arises during or results from “fundamental research” is not subject to the EAR, not all university research falls under this exclusion. For example, as is often the case when companies fund university research projects,⁵² any non-disclosure agreement or proprietary component would preclude publicly available treatment. If foreign nationals are not allowed to work on these projects, it will limit commercial funding of academic research, a key way that professors and graduate students are funded. These restrictions would severely impact not only U.S. cybersecurity, but academia and science and technology research more broadly.

3. U.S. Companies Outside of the Cybersecurity Industry

In addition, a broad range of U.S. companies that are consumers of cybersecurity technologies would face the burden of deemed export restrictions, many for the first time. The impact of this rule would be vast.

⁵¹ According to a 2013 report by the National Foundation for American Policy (“NFAP”), foreign students (who are not lawful U.S. permanent residents), make up 70.3% of full-time graduates in electrical engineering and 63.2% of full-time graduates in computer science. Stuart Anderson, NFAP, *The Importance of International Students to America* at 1-2 (July 2013), available at http://www.councilforglobalimmigration.org/ADV_NFAP_Report_July_2013 (“Foreign graduate students are crucial in assisting in research that attracts top faculty and strengthens the academic programs at U.S. schools, which benefits U.S. students and ensures America retains its preeminence as a teaching center in science, technology, engineering and math (STEM) fields.”).

⁵² For example, the University of Idaho, Center for Secure and Dependable Systems (“CSDS”) “works with companies and government agencies to analyze and design software that safeguards computer infrastructure.” Ysabel Bilbao, *Staying Well Ahead of Hackers and Protecting the Public*, CSDS, University of Idaho, <http://www.uidaho.edu/engr/csds/projects/staying-ahead-of-hackers>. See also Cybersecurity Research, Center for Cybersecurity, University of South Florida, <http://www.usf.edu/cybersecurity/research/> (“USF has a long and successful record of securing federal and industry funding. . . .”); Cybersecurity Research, Seidenberg School of Computer Science and Information Systems, Pace University, <http://www.pace.edu/seidenberg/cybersecurity/research> (“Skimmer Fraud Research funding has been provided by Association of Chartered Certified Accountants.”). Ionic is also currently planning collaboration on a research project with Dartmouth College, as well as sponsorship of a senior research project at Georgia Institute of Technology, University of Tulsa, University of Illinois Urbana-Champaign, or Dartmouth College.

D. Intracompany Transfers

The absence of a license exception for intra-company transfers or internal use⁵³ is highly problematic given the breadth of the restrictions. This may preclude multinational companies from purchasing U.S.-origin cybersecurity products, because of the globally integrated nature of their networks. The favorable licensing policy for certain intracompany transfers would not be enough to bring those customers back, both because of the very existence of a licensing requirement, and because it would not apply to countries such as Russia and China where cybersecurity needs are great. Companies prefer integrated solutions and would be very reluctant to use a provider whose product would be restricted in countries like China and Russia. While the intent of this policy is to prevent transfers of controlled technology to these countries, the effect would be the opposite, depriving U.S.-based companies of their best defenses where they are the most vulnerable. Often attackers only need to find the weakest link in a network to access its systems, so good protection in one country is of little value if it does not apply in another country. For this reason, customers may begin to prefer a non-U.S.-origin product that they can use enterprise-wide.

IV. THE PROPOSED RULE IS BROADER THAN WASSENAAR REQUIRES

In light of its impact on cybersecurity, it would be prudent for BIS, at a minimum, to restrict the proposed rule to the scope required by the Wassenaar Arrangement. However, there are areas in which the proposed rule appears to control a broader scope of cybersecurity items than other Wassenaar countries' analogous rules and imposes more stringent licensing requirements. For example, while Wassenaar and the European Union control lists use the same definition for "intrusion software" and the same categories for new items, the U.S. proposed rule arguably goes further by explicitly including network penetration testing products and proprietary research on vulnerabilities and exploitations, and stating a license policy of presumptive denial for items that have "rootkit" and "zero-day" exploit capabilities.

Additionally, as a practical matter, it appears the EU regulations have so far not been enforced as strictly as the U.S. proposed rule likely would be. For example, Hacking Team is an Italian firm that offers hacking tools and support to foreign governments, including tools that use malware. In the United States, licenses for such products would only be favorably viewed for a few countries. In the European Union, however, according to documents revealed in a recent hack of Hacking Team, the company was supporting sales of malware exploitation to numerous governments, including, but not limited to, Egypt, Ethiopia, Nigeria, Sudan, Malaysia, Bahrain, Vietnam, Saudi Arabia, Oman, and the UAE. And the company said in their leaked emails that their product is covered by Wassenaar, that it submitted license applications to the Italian government for sales to new customers (including a global authorization to allow export freely in all Wassenaar countries), and that it is in compliance with export control laws including the recently imposed Wassenaar protocols. Since it has continued its services, it has presumably obtained all of these licenses—an unlikely result under the U.S. proposed rule. The U.S. government should not impose the Wassenaar rule in a way that disadvantages its own companies.

⁵³ See FAQ #17.

A. Differences in the Applicability of the General Software Note and Mass Market Exception to Cybersecurity Items

A clear example of the United States applying stricter controls than the EU, Canada, and Australia is how the controls on “mass market” cybersecurity items will be implemented. In the United States, under the proposed rule, cybersecurity items are not eligible for either the “mass market” license exception or the lesser-controlled ECCN available for “mass market” encryption items (ECCNs 5A992, 5D992, and 5E992).⁵⁴ By contrast, under Wassenaar, and as implemented in the EU, Canada, and Australia, cybersecurity items without encryption appear to be eligible for exclusion under the General Software Note’s “mass market” provision, and, if they incorporate encryption they are still eligible for decontrol under the Cryptography Note (Category 5, Part 2, Note 3).⁵⁵

By including mass market items specifically excluded under Wassenaar and other countries’ implementing regulations, the U.S. proposed rule would require licenses for a broader scope of items than other Wassenaar countries. Such products could include Metasploit (Metasploit Pro), which is a penetration testing software that is openly sold in near retail fashion.⁵⁶

BIS’s rationale for this broad scope—that it is necessary for consistency with the existing treatment of encryption items⁵⁷—is not convincing. Cybersecurity items do not all have or need encryption capabilities, and the export of cybersecurity items, especially those without encryption, should not suffer from an overbroad attempt at “consistency.” Additionally, despite BIS’s assertions, the proposed rule does not treat encryption items and cybersecurity items consistently. It imposes heavier restrictions on all cybersecurity items (with or without encryption) than on encryption items themselves. At the very least, if cybersecurity items with encryption functionality are to be controlled consistently with existing encryption regulations, the “consistency” should extend to *both* the restrictions *and* their eligibility for license exceptions and less restricted ECCNs.

⁵⁴ See *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. at 28857 (to be codified at 15 C.F.R. § 740.13(d)(2)); see also FAQs #23, #31.

⁵⁵ See *The Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List* at 3, 86 (March 25, 2015) (hereinafter “Wassenaar List”); see also Commission Delegated Regulation (EU) No. 1382/2014, 2014 O.J. (L 371) at 4, 141 (Oct. 22, 2014) (“hereinafter EU No. 1382/2014”); *A Guide to Canada’s Export Controls* at 1, 78 (Dec. 2013) (“hereinafter “Canada’s Guide”); *Australia, Defence and Strategic Goods List* at 62-63, 212-213 (April 8, 2015) (hereinafter “Australia’s List”).

⁵⁶ Other examples of mass market products are penetration testing software offered by Cobalt Strike (<http://www.advancedpentest.com/>) and Core Security (<http://www.coresecurity.com/core-impact-pro>), as well as similar tools that automatically generate and deliver exploits to verify vulnerabilities, such as Acuetix WVS (<http://www.coresecurity.com/core-impact-pro>) and NetSparkler (<https://www.netsparkler.com/web-vulnerability-scanner/false-positive-free-web-security-scan/>).

⁵⁷ See FAQs #23, #31.

B. Differences in the Applicability of the Exceptions in the General Technology Note to Cybersecurity Items

The General Technology Note is also implemented differently in the United States than in other Wassenaar countries. In the EU, Canada, and Australia, the General Technology Note, as under Wassenaar, provides that “[c]ontrols do not apply to that ‘technology’ which is the minimum necessary for the installation, operation, maintenance (checking) or repair of those items which are not controlled or whose export has been authorised.”⁵⁸ There does not appear to be a limitation in applying this provision to cybersecurity technology. In the United States, however, this General Technology Note provision is implemented through License Exception TSU,⁵⁹ which is not available for cybersecurity items.⁶⁰ BIS should not apply different treatment than other Wassenaar countries in this way.

V. INCONSISTENCIES WITH OTHER SECURITY COMPLIANCE REGIMES AND INFORMATION SHARING INITIATIVES

Additionally, the numerous federal data protection requirements and information sharing initiatives⁶¹ are in direct tension with the proposed rule, which restricts the ability of companies to use necessary tools for data and network protection and restricts the flow of information about cybersecurity tools.

A. Financial Industry

1. Gramm–Leach–Bliley (GLB) Act⁶²

For example, the GLB Act has numerous data protection requirements, which could be more complicated for companies to implement under the proposed rule. It requires “financial institutions”⁶³ to ensure the security and confidentiality of information they collect about

⁵⁸ Wassenaar List, General Technology Note, at 3; *see also* EU No. 1382/2014 at 4; Canada’s Guide at 1; Australia’s List at 62.

⁵⁹ *See* 15 C.F.R. Part 774, Supp. No. 2 (“License Exception TSU is available for “technology” that is the minimum necessary for the installation, operation, maintenance (checking), or repair of those products that are eligible for License Exceptions or that are exported under a license.”).

⁶⁰ *See Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28856-57 (to be codified at 15 C.F.R. § 740.2(a)(19)).

⁶¹ While these comments focus on relevant federal requirements, there are similar individual state requirements for data protection that may also be implicated by the proposed rule. For example, Massachusetts regulations impose security standards for the possession, licensing, storage and transmission of personal information about state residents that must, at a minimum, include reasonably up-to-date versions of system security agent software with malware protection and reasonably up-to-date patches and virus definitions, and the receipt of current security updates on a regular basis. Mass. 201 CMR 17.00, Section 17.04.

⁶² P.L. No. 106-102 (Nov. 12, 1999).

⁶³ This includes not just banks, but also insurance companies, financial advisers, nonbank lenders, loan brokers, tax preparers, providers of real estate settlement services, appraisers, courier services, ATM operators, credit reporting agencies, and debt collectors. The FTC is one

individual consumers, under the “Safeguards Rule.”⁶⁴ Specifically, it requires financial institutions to develop, implement and maintain “reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information”⁶⁵ and “a comprehensive information security program that . . . contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.”⁶⁶ For large institutions, complying with these data requirements often involves extensive penetration testing that is in line with industry standards, but would be controlled under the proposed rule.

The GLB Act also requires financial institutions to “[d]esign and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.”⁶⁷ The risk assessment should cover “[i]nformation systems, including network and software design, as well as information processing, storage, transmission and disposal.”⁶⁸ It also instructs financial institutions to “[e]valuate and adjust your information security program in light of the results of the testing and monitoring.”⁶⁹ Again, to satisfy these requirements for “risk assessment” in line with industry standards, large institutions often engage in penetration testing that would be captured by the proposed rule.

The GLB Act also requires financial institutions to take steps to ensure that affiliates and service providers safeguard customer information as well.⁷⁰ FTC guidance⁷¹ suggests specific information security measures, many of which could be complicated by the proposed rule, including:

- Keep logs of activity on your network and monitor them for signs of unauthorized access to customer information;

of eight federal regulatory agencies that has the authority to enforce the financial privacy law, along with the state insurance authorities. The federal banking agencies, the Securities and Exchange Commission and the Commodity Futures Trading Commission have jurisdiction over banks, thrifts, credit unions, brokerage firms and commodity traders.

⁶⁴ This FTC rule applies to all businesses, regardless of size, over which the FTC has jurisdiction that are “significantly engaged” in providing financial products or services. *See* GLB Act §§ 501, 505(b)(2); 16 C.F.R. Part 314, 67 Fed. Reg. 36,493 (May 23, 2002).

⁶⁵ 16 C.F.R. § 314.1(a).

⁶⁶ *Id.* § 314.3(a).

⁶⁷ *Id.* § 314.4(c).

⁶⁸ *Id.* § 314.4(b)(2).

⁶⁹ *Id.* § 314.4(e).

⁷⁰ *Id.* §§ 314.2(b), 314.4(d).

⁷¹ *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, Federal Trade Commission (April 2006), available at: <https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying>.

- Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- Insert a dummy account into each of your customer lists and monitor the account to detect any unauthorized contacts or charges.
- Use an up-to-date intrusion detection system to alert you of attacks;
- Maintain up-to-date firewalls;
- Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
- Use antivirus and antispyware software that updates automatically;
- Use a Secure Sockets Layer (SSL) or other secure connection when transmitting credit card information or other sensitive financial data to protect the information in transit; and
- Encrypt sensitive data if it must be transmitted by email.

The proposed rule would complicate companies' ability to comply with the GLB Act's mandate to use intrusion detection systems, monitor network activity, and test the security features of their network and software design and data storage and transmission procedures. Imposing export controls on products designed to operate, deliver or communicate with intrusion software would make it more complex for companies to use intrusion detection systems as required by the GLB Act, because as discussed throughout these comments these testing and defensive tools often must operate, deliver, or communicate with intrusion software. In particular, the proposed rule would complicate these companies' ability to conduct comprehensive testing on their networks, software and hardware, if they were restricted in their ability to use those systems across the entire company network (including facilities overseas) or to allow access by foreign national employees or service providers. Even if made workable by revisions to the proposed rule, imposing a BIS licensing requirement on top of an FTC information security obligation would present an undue burden for many small companies. Similarly, the proposed controls on IP surveillance systems may conflict with the GLB Act's requirement to monitor network traffic.

2. SEC and FINRA

Relatedly, Rule 30 of SEC Regulation S-P (referred to as the "Safeguard Rule")⁷² requires every broker, dealer, investment company and registered investment adviser to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information . . . reasonably designed to:

1. Insure the security and confidentiality of customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
3. Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

⁷² 17 C.F.R. § 248.30(a), 65 Fed. Reg. 40,362 (June 29, 2000), amended by 69 Fed. Reg. 71,329 (Dec. 8, 2004).

The proposed rule would limit companies' access to the types of tools they need in order to comply with these mandates.

B. Payment Cards

The Payment Card Industry Data Security Standard ("PCI DSS") is a set of security standards to which major credit card companies have agreed to adhere and to enforce against merchants. The PCI DSS are applied against all organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any cardholder data, essentially any merchant that has a Merchant ID ("MID").⁷³ Under the newly released PCI DSS 3.0 and 3.1, any business that stores, processes or transmits payment cardholder data **will need to perform penetration testing** based on industry standards.⁷⁴ Such testing is required at least on an annual basis and after any significant change in the network infrastructure or applications. But the tools to do this testing may not be as accessible under the proposed rule because licenses will be required for multinational companies to use penetration testing tools from U.S. companies throughout their global networks.

C. HIPAA (HITECH)

Similarly, the Health Information Technology for Economic and Clinical Health ("HITECH") Act requires the protection of data in the electronic transmission of health information and strengthens the civil and criminal enforcement authorities of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in this area.

The HITECH Act provides for the creation of a National Coordinator for Health Information Technology within the Department of Health and Human Services and requires the holder of that office to include specific objectives, milestones and metrics with respect to: the incorporation of privacy and security protections for the electronic exchange of an individual's health information; and ensuring security methods to ensure appropriate authorization and electronic authentication of health information and specifying technologies or methodologies for rendering health information unusable, unreadable, or indecipherable.⁷⁵

The proposed rule, by restricting cybersecurity products, would make compliance with such requirements more difficult for multinational companies, who must provide these protections throughout their global networks.

⁷³ See generally PCI Security Standards Council, *available at*: <https://www.pcisecuritystandards.org/index.php>; see also *PCI FAQs*, PCIComplianceGuide, ControlScan, *available at*: <https://www.pcicomplianceguide.org/pci-faqs-2/#2>.

⁷⁴ See *Information Supplement: Penetration Testing Guidance*, PCI Security Standards Council (March 2015), *available at*: https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf.

⁷⁵ Pub. L. No. 111-5 (Feb. 17, 2009), Section 3001.

D. Other U.S. Export Control Requirements

The proposed rule is also inconsistent at a broad level with the recent proposed rules from BIS and DDTC⁷⁶ offering a safe harbor from export controls when information transmitted or stored abroad in electronic form is protected by adequate end-to-end encryption. While on the one hand recognizing the importance of strong security features like encryption to the successful operation of an international business, BIS has proposed new controls that would restrict access to and development of similar critical technologies. Some components of an end-to-end encryption solution, which BIS relies on for the effectiveness of its new safe harbor provision, would in some cases be subject to the intrusion software controls and thus would be less widely available and subject to innovation-stifling licensing requirements. For example, the Ionic products described above encrypt data wherever it goes and allow access restrictions to be set by location (such as to disallow access from outside the United States), so they may be among the products that would both be useful in implementing BIS's envisioned export safe harbor but also restricted under the proposed rule. Consistent with the approach BIS took in crafting the encryption safe harbor, the U.S. government should recognize the paramount importance of world-leading cybersecurity capabilities.

Similarly, License Exception TMP, 15 C.F.R. § 740.9, and other provisions of the EAR already require the protection of data. License Exception TMP requires that software used as a tool of trade be "protected against unauthorized access," including with secure connections, passwords and firewalls. Under License Exception TMP, the exporting, reexporting, or transferring party and the recipient of the technology must take security precautions to protect against unauthorized release of the technology. Such requirements are inconsistent with limiting access to the equipment, software, and technology that could provide such protection.

E. U.S. Government Information Sharing Initiatives

The proposed rule also conflicts with the priority placed on information sharing by both the Administration and Congress, for instance, the numerous information sharing programs developed by the Department of Homeland Security,⁷⁷ and those in the Intelligence Community.⁷⁸ The rule would severely restrict information sharing in the cybersecurity industry by imposing sweeping licensing requirements and restrictions on access to information by foreign nationals and by persons outside the United States. For instance, the Industry Consortium for Advancement of Security on the Internet ("ICASI") is a trusted private forum for internet companies to proactively collaborate to analyze, mitigate, and resolve multi-stakeholder,

⁷⁶ *Revisions to Definitions in the Export Administration Regulations*, 80 Fed. Reg. 31505, 31517 (June 3, 2015); *International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions*, 80 Fed. Reg. 31525, 31537 (June 3, 2015).

⁷⁷ See, e.g., U.S. Department of Homeland Security, Cybersecurity, Information Sharing, <http://www.dhs.gov/topic/cybersecurity-information-sharing>.

⁷⁸ See, e.g., *Strategic Intent for Information Sharing 2011-2015*, Office of the Director of National Intelligence, available at: <http://www.dni.gov/files/documents/Strategic%20Intent%20for%20Information%20Sharing.pdf>.

global security challenges. ICASI is not a fully open forum,⁷⁹ so the BIS rule may restrict its ability to operate effectively.

VI. CONSEQUENCES OF THE PROPOSED RULE

As discussed herein, the proposed rule would control defensive tools that companies use to keep their own software, networks, and infrastructure safe. Such broad controls of legitimate defensive products would negatively impact cybersecurity, chill research and innovation, and disadvantage the development of cybersecurity solutions in the United States. Information sharing and collaboration are the foundation of an effective cybersecurity industry. The proposed licensing policies would shatter that foundation and make continued research and development, and security operations, nearly impossible to conduct in the United States.

A. Companies' Ability to Protect Their Own Networks

The result of these broad controls would be to make it more difficult for cybersecurity companies to protect their customers and the general public from cyber-attacks. Restricting access to the cybersecurity tools discussed in these Comments could weaken the security of companies and their products, while doing little to stop the use of these tools. By prohibiting even the intracompany transfer of cybersecurity items, these rules complicate the use of such items for protective or testing purposes by U.S.-based multinational companies and their foreign subsidiaries. Additionally, due to the rule's overbroad restrictions and ambiguities, legitimate activities, such as threat intelligence sharing (which often discusses the technology and tactics of the adversary's intrusion software) and security research on attack techniques, may be regulated and discouraged. Such information sharing and research is essential to create better software and defense mechanisms. Harsh regulation could result in fewer vulnerabilities found and shared, fewer fixes and defenses made, and ultimately less secure systems. And if research and international collaboration are discouraged in the United States more than elsewhere, the United States' leadership and expertise in this field will atrophy, putting the United States at a distinct security disadvantage.

For example, the proposed rule would affect the ability of multinational companies to communicate and share information internally to develop protections. Companies have to go through many steps to develop defenses, including testing their systems for vulnerabilities, developing exploits to more fully understand and prioritize the vulnerabilities, sharing this information with vendors to collaborate in developing a defense to secure the system, and developing and using a system for efficiently delivering the defense into the existing product. The proposed rule appears to require licenses at every step. These extreme restrictions would halt companies' ability to go through the steps of fixing vulnerabilities.

Additionally, companies' research teams are finding these vulnerabilities and writing these exploits in real time. When a vulnerability is discovered, the process begins

⁷⁹ ICASI says on its website that it engages in "selective expansion of membership" and collaborates with "targeted industry groups and other bodies so that trust among members and participants is maintained." See *Our Mission & Goals*, ICASI, available at: <http://www.icasi.org/our-mission/>.

immediately—the idea of having to wait for a license is a non-starter. It is not even a matter of days, but minutes, usually just a few minutes. The company engages right away in a back-and-forth dialogue with outside experts, who may be non-U.S. persons and may not have (or ever form) a formal relationship with the company. Even if the company’s primary security provider is the beneficiary of some kind of blanket license, the third parties that the security provider may need to bring into the process likely would not be. This entire process of patching a vulnerability needs to be completed within days in order to prevent its exploitation by malicious actors. However, this entire process would be subject to licensing requirements under the proposed rule, which is clearly not workable no matter how liberal the licensing policies. Ultimately, these controls would leave companies and the public, both within and outside the United States, much more vulnerable to attack and unable to respond effectively.

B. Security Research and Innovation

Probably no other industry relies as heavily on daily, real-time innovation as the cybersecurity industry—it is constant and relentless. The breadth and ambiguity of the proposed rule would also have a profound chilling effect on the research and development of critical cybersecurity items.

Cybersecurity research teams, in companies and academia, work on a wide variety of projects that involve techniques that would be caught by the proposed rule. An example of the type of innovation that would be precluded in the future under the proposed rule is BlackIce, one of the early network defense technologies for Windows. BlackIce was not made by Microsoft, but worked by hooking into Windows, diverting and modifying its path of execution in order to provide its security functionality. It used an innovative technique that had not been used before. If the developers had been restricted by regulations similar to the proposed rule, it would have never been developed. As discussed above in Section II.B.2.c, almost all software innovation requires “modifying the standard execution path” of a program because it involves building on and improving other people’s software in ways they did not contemplate or intend when they wrote it. Therefore, the proposed rule would chill innovation across the entire software industry, not just in cybersecurity.

In the cybersecurity community, communication is key to innovation. If researchers in the United States cannot quickly and efficiently communicate with researchers in other countries, they would be cut off from this global community and would fall behind their peers. Such communication cannot be limited to merely providing samples as BIS has proposed—it must dive into the details of the technology that was required to find the vulnerability and generate the exploit. Even within companies, the proposed rule would seriously impede the ability to work and collaborate with colleagues abroad and foreign nationals in the United States on the development of more secure products and addressing current threats.

A clear example of this is sharing exploit toolkits, which are tightly controlled by malicious actors, who aim to prevent good actors from getting ahold of them and tailoring countermeasures for them. Exploit toolkits themselves allow bad actors to easily deliver exploits to a system, and upgrades and additional exploits can be added to a toolkit. These toolkits come ready and easy to use, with all of the tools to operate, deliver, and communicate with the exploits. There is an entire underground business which has been built around such toolkits to

aid exploitation. While it may be desirable to control malicious actors from using and sharing these toolkits, as a practical matter, the proposed rule will not stop sharing by malicious actors, who will continue to share these toolkits, including on the black market and outside the United States. What the proposed rule would do instead is prevent law-abiding security professionals from quickly and effectively providing defenses for such toolkits. As a practical matter, when a security professional manages to get ahold of such a rare toolkit, it is the practice to share it with other security companies with which there are formal or informal mutual sharing agreements (including internationally) in order for these companies to develop defenses. Because these toolkits include not just exploits but also the entire framework for delivering and communicating with them, they clearly fall into the regulated categories. But to create defenses, companies frequently need to share the entire toolkit (not only the exploits, but the tools in the kit used to operate, deliver, and communicate with the exploits) to learn how the toolkit hides, protects, and delivers its exploits. By preventing companies from sharing this information, the proposed rule would make it much more difficult for defensive companies to access these offensive tools in order to test and defend against them.

The effects the proposed rule would have on FireEye's threat intelligence sharing efforts are another example of its negative repercussions. FireEye anonymously exchanges data on email, web and file based threats on an hourly basis across its global customer base via its Distributed Threat Intelligence (DTI) cloud. This ensures that FireEye customers are protected against the most recent attacks FireEye has seen across its global customer base. This data may include technical indicators, contextual information, malware command and delivery tools, malware samples and other data that provides a clear picture of the malware infrastructure, capabilities and methodologies used by the attackers. The more extensive these descriptions of the exploit and the richer the pool of data, the better the defenses that FireEye is able to provide to its customers. If FireEye is unable to share this threat intelligence in near-real time across borders, FireEye customers, including many federal, state and local government customers, would not be protected from the most recent cyber-attacks. This situation would leave organizations unnecessarily vulnerable to exploitation.

FireEye also shares data with other companies and research labs to enhance the collective defense of the community at large. If this information were not able to cross borders, it would cripple this type of intercompany dialogue, as well as FireEye's and other U.S. companies' internal processes. If that were to occur, the United States would be left out of cutting-edge cybersecurity research and development.

C. Effectiveness of the U.S. Cybersecurity Industry

It is in the United States' security interests to have a strong and vibrant U.S. cybersecurity industry, so to have access to expertise and cutting edge defenses within its own shores. It should be an industry that the United States invests in and encourages. But the proposed rule would stymie the development of the cybersecurity industry in the United States, causing U.S. capabilities to lag behind those in countries with less onerous restrictions and ultimately come to depend on them for its cybersecurity needs. The proposed rule would act as a direct restraint on U.S. cybersecurity companies with a global presence, who use resellers, channel partners, and a network of sales and marketing agents around the world, not to mention their own foreign national employees and research partners and overseas facilities. But it would

also restrict cybersecurity companies' ability to sell their products even within the United States. Multinational companies want products they can use enterprise-wide, and putting a restriction on the use of U.S.-origin products may act as a complete barrier to contracts with these companies. Cybersecurity companies, which depend on rapid information-sharing to remain competitive, would be encouraged to minimize their presence in the United States.⁸⁰ In this way, the proposed rule would severely hamper the development of cybersecurity defenses in the United States, while driving that expertise to our strategic competitors.⁸¹

D. Ineffective in Controlling Malicious Intrusion Software and Surveillance Items

Although the proposed rule would be certain to damage the cybersecurity of the United States, it would not accomplish its goal of controlling the malicious use of intrusion software and surveillance items. First, unlike other highly regulated industries, the cybersecurity community does not operate in organized teams under a corporate parent. Malicious actors in this realm can act independently—all they need is a computer—and from anywhere in the world. Licensing requirements, while likely to stop or slow the law-abiding defenders, would have very little effect on the activities of malicious actors. Malicious tools will continue to be widely available on the black market or from China or other non-Wassenaar countries (and possibly even other Wassenaar countries like Russia), because “exporting” lines of code requires only seconds of access to the internet.

Additionally, the controls themselves, even if implemented seamlessly, would be ineffective in preventing the generation, operation or delivery of, or communication with, malware. The reason is simple: almost any software can be used for those purposes. As discussed above in Section III.B.2.a, generic delivery tools can be used to deliver malware into a system. Additionally, normal websites may be used for “Command and Control” (“C2”) for intrusion software, which includes operation, communication, and potentially delivery. For example, malware has used, without any modifications required, Google Docs, various email

⁸⁰ BIS should take care to not repeat the mistakes of the cryptography controls put in place in the 1990s, which were a major impediment to the development of security technology in the United States.

⁸¹ Many of these countries are already competitive in this realm, but the proposed rule would shift the competitive landscape very significantly in their favor. In China, where there is a growing market for such products, companies are increasingly investing in these areas. For example, Sempian Technologies, Ltd, a Chinese network solutions company with the slogan “cyber monitoring expert,” is starting to develop more sophisticated IP network surveillance equipment. The same is true in Israel. Examples include: ECI Telecom Ltd. (an Israeli company that delivers comprehensive networking to service providers); Hybrid Security (an Israeli cyber software vendor, whose Telepath product automatically learns typical user behavior patterns within web applications); Netline Communications Technologies (an Israeli company that specializes in communication jamming and detection systems and sells products including cell phone interception and RF monitoring); Votiro Inc. (an Israeli company that develops software packages to protect networks and IP infrastructures); White-Hat Ltd. (an Israeli penetration testing firm that does cyber defense consulting, 24/7 response, and penetration testing). All of these companies would benefit from decreased competition from U.S. companies and pushing cyber expertise outside of the United States.

services, and other legitimate websites and services for C2 purposes when trying to access a system. Though some malware may be made with specialized tools, most intrusion software is “generated” with tools that developers worldwide use every day (i.e. standard software development environments and coding languages). Using such standard tools for malware attacks is in fact advantageous for malicious actors because protective countermeasures cannot single out such tools as easily, so they tend to leave a smaller trace.

Even if there does exist a small number of U.S. companies both whose tools would be captured under the proposed rule and who sell these tools to bad actors, these companies can easily and immediately move underground or offshore, resulting in no real security benefit. And the U.S. government must ask itself if catching and denying one or two license applications from bad actors, who will continue to sell their products either by simply not applying for a license the second time around or by moving offshore, is really worth the drastic decrease in the United States’ cybersecurity abilities that it would cause and the resources for Commerce to issue the thousands of licenses it would necessitate.

The problems we have laid out above are only illustrative. The larger point here is that the proposed rule is unworkable and it will be virtually impossible to fix it within its current structure. Our hope is that the comments BIS receives in response to this proposed rule will make clear to the government what is already painfully apparent to industry—that it is extremely difficult to craft export control regulations in this sector that will account for its complexity and dynamism. The very existence of a licensing regime, even with broad and liberal license exceptions, would greatly discourage and hinder the U.S. cybersecurity sector. Because this export control licensing regime would also have very little effect on the transfer of malicious malware, it would be advisable to return to Wassenaar to attempt to draft a regulation that is better suited to accomplish its goals and better targeted to not capture legitimate cybersecurity efforts.

VII. PROPOSED SOLUTIONS

The fundamental framework of the proposed rule is critically flawed and cannot be fixed with a few simple changes. Below, the Coalition has laid out a few ideas that could be more effective in addressing the problem of malicious cyber activity, as well as some suggestions for ways the proposed rule may be made somewhat less harmful to industry. However, the Coalition feels the best option would be for the U.S. government to return to Wassenaar early next year to rework the 2013 agreement if it wants to correct the significant problems with this proposed rule.

The fundamental problem is the idea of imposing traditional export controls based on classification and destination on cybersecurity items. That approach will have a massively disproportionate impact on legitimate actors, far more so than in other industries. The cybersecurity sector is unique in part because bad actors operate almost entirely electronically, and are not easily subject to monitoring for compliance with a Commerce Department licensing requirement, and the good actors rely so heavily on speed, flexibility, international scope and information sharing that any licensing regime, no matter how it is structured, would stymie their effectiveness.

Moreover, U.S. companies are heavily dependent on the expertise of a mobile and global community of independent operators and losing access to them would mean that U.S. companies would be unable to stay on top of the threat environment. In this industry, the difference between being one step ahead and one step behind is everything. If our companies lose that critical edge, U.S. cybersecurity will be at risk. And the global community of independent operators—if they were made subject to a licensing requirement, or forced to share their data with the U.S. government—would simply opt out and drop back into the shadows. They are not like traditional manufacturers, for instance, who are part of the formal global economy, and therefore have to submit to whatever regulatory requirements are imposed on them. Instead, these individuals often make a living informally, and are more than capable of doing so. We hope that the U.S. government will take account of these important factors that make this industry unique, and craft a regulatory regime around this reality, rather than trying to shape the world to fit its rules, because this world is formless and cannot be squeezed into a box.

Finally, the U.S. government and the U.S. economy, along with the rest of the world, rely heavily on the U.S. cybersecurity industry, and they are expected to come to rely on it even more with time in order to stay secure and competitive in the digital age. We hope that policy makers will get serious about this issue while the door is still open, and redirect their efforts towards a productive path. Below we sketch out the contours of such a path.

A. Solutions That May Work

As described below, we believe that tinkering with the current proposed rule will not work. However, we will first briefly mention a few ideas for how the problem of malicious cyber activity may be addressed in a more effective way.

1. Criminal Law

One tool to counter malicious cyber activity, and the one with the least likelihood of having damaging side effects, would be the general criminal law.⁸² Rather than spinning its wheels on the currently proposed rule, the U.S. government should dedicate these resources to an existing capability that will work: the FBI and federal prosecutors. While the Commerce Department does have investigative capabilities, it has far less experience in the cyber realm than the FBI and Justice Department, and cannot bring the same kinds of tools, global resources and

⁸² An example of criminal prosecutions in this area include the recent international takedown of the Darkode forum, a marketplace to purchase and trade malware and hacking tools. This takedown involves arrests in 20 countries and indictments of 70 individuals, including 12 in the United States. Bill Chappell, *Malware and Hacking Forum Darkode is Shut Down; Dozens Arrested*, NPR (July 15, 2015), <http://www.npr.org/sections/thetwo-way/2015/07/15/423196810/malware-and-hacking-forum-darkode-is-shut-down-dozens-arrested>. Another example involves a Pakistani man who was indicted for conspiring to advertise and sell StealthGenie, a spyware application that could monitor calls, texts, videos, and other communications on mobile phones without detection. *Pakistani Man Indicted for Settling StealthGenie Spyware App*, Washington Field Office, Federal Bureau of Investigation (Sept. 29, 2014), <https://www.fbi.gov/washingtondc/press-releases/2014/pakistani-man-indicted-for-selling-stealthgenie-spyware-app>.

expertise to the table. BIS is skilled at regulating the noncompliant side of normal commerce. The FBI specializes in underground criminal activity. The problem with malicious cyber-attacks and intrusions of privacy does not stem from noncompliant or unethical U.S. companies—it is a problem that is based largely overseas and works with underground criminal networks and abusive foreign governments. Those are not threats that BIS is well-suited to address. To the extent there is a small portion of this threat that relies on U.S. companies, that portion would easily and immediately move offshore and this proposed rule would be worth no more than the paper it was written on as soon as it was issued (although its negative effects would persist).

2. Sanctions

In tandem with criminal law enforcement, the U.S. government can tackle this threat through trade sanctions, including so-called “secondary” sanctions that apply to non-U.S. persons. The Treasury Department’s Office of Foreign Assets Control (“OFAC”) is already engaged in this area. Executive Order 13,694 (April 1, 2015) provides for blocking all property and interests in property within U.S. jurisdiction of “persons” determined to have engaged in “cyber-enabled activities” occurring “in whole or in substantial part” outside the United States that may constitute a significant threat to the “national security, foreign policy, or economic health or financial stability of the United States” and that have the purpose or effect of:

- (A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
- (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
- (C) causing a significant disruption to the availability of a computer or network of computers; or
- (D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain.”

That order also separately covers activities involving “trade secrets misappropriated through cyber-enabled means.”

OFAC can play a significant role in supporting criminal law enforcement efforts by dedicating more resources to implementing this order. To-date, no designations have been made under Executive Order 13,694, so its deterrent effect has been limited.

3. Part 744.6 Controls

It may also be possible for BIS to play a productive part in this effort, but it cannot look anything like the role envisioned under the current proposed rule. We will set out a few ideas below with the goal of sparking a more productive conversation on this topic, but we have to preface this section by underscoring that the very short comment period has not afforded us sufficient time to fully consider precisely how these controls would work or what their impact would be. We hope that the next proposed rule from BIS will bear little resemblance to the

current proposed rule, in which case that may be a good time to discuss more palatable solutions in more detail.

It may be possible, for instance, for these controls to be crafted as Part 744.6 restrictions on activities of U.S. persons. Like the existing Part 744.6 controls, the proposed rule targets a broad set of items but only when used in very narrow ways, though ways that would have a profoundly dangerous impact. The existing Part 744.6 controls target transactions involving *any item* intended for the proscribed end-uses: nuclear explosive devices, missiles, or chemical or biological weapons. That is a good model for the cybersecurity controls, because nearly any software product or method can be used maliciously to steal data or invade privacy, as we hope we adequately demonstrated in the preceding sections. These are not controls that would be effective by attempting to spell out particular capabilities or technical characteristics. Any effort to target specific items will always be both underinclusive (by failing to keep up with new ways that bad actors operate) and overinclusive (by sweeping in legitimate defensive tools), and it would be a mistake to underestimate how innovative cyber operators can be in coming up with completely new ways of achieving their goals.

Furthermore, controls modeled on Part 744.6 make sense here because they are based on knowledge. As discussed at length in the preceding sections, the only distinction that can be made between many types of necessary defensive cyber products and malicious tools is the intent of the user. That end-use intent is exactly what Part 744.6 targets. A control regime based on knowledge and end-use will be more adaptive and more effective—and less of a drain on regulatory and enforcement resources—because it has the advantage of focusing directly on the actual ends (stopping malicious cyber activity) rather than employing a flawed focus on the means (systems, software, and tools that are capable of being used for both malicious and defensive purposes). Moreover, under this approach, BIS would not have to struggle to constantly revise the regulations to account for the new technological developments that are a constant in this industry. BIS is likely to always lose that race; and it is probably not a race they want to be in. Part 744.6 requires every manufacturer, exporter, trader, shipper and facilitator to conduct due diligence in any transaction involving red flags indicating possible unlawful end-uses. The people that live in this world are the most well-suited to spot the threats. Even more, cybersecurity companies have the most at stake here and would be active partners in this effort, provided that the regulatory regime takes account of how this industry works. Their business relies completely on their reputation with their customers and the integrity of their systems. If their products were diverted to malicious groups, they would lose their customers' trust and lose their business. A regime focused on due diligence rather than a constant churn of pointless license applications would make sense. And it would be transformative from a law enforcement perspective: a panopticon of cybersecurity companies always watching for diversion would be exponentially more effective than a BIS licensing officer wondering why he still hasn't seen an application from the bad guys.

A control regime structured like Part 744.6 would match the global nature of this threat. Rather than crafting different country-based licensing policies when malicious cyber threats emanate from anywhere and everywhere, this approach focuses on the particular threat profile (intent and capability) of the end-user. Again, rather than putting the responsibility on a BIS licensing officer to decide whether a sale to a little-known company in Estonia, for example,

should be permitted, and rather than making BIS constantly update its geographical licensing policies based on new threat intelligence, it would make more sense for the people on the ground to make that call, at the risk of facing liability, and losing their business. In cases when the government does have the relevant information to play a useful role, Part 744.6(b) has a built-in provision for special controls upon notice to the person concerned.

This type of control would also have the desired scope: it would cover activities by foreign nationals in the United States, U.S. citizens and residents anywhere in the world and U.S. companies and their foreign branches. Furthermore, Part 744.6 controls can extend to support activities such as financing and other facilitation, as well as performing any contract, service or employment that the U.S. person knows will directly assist in the proscribed activity.⁸³

The Coalition welcomes a conversation about whether controls modeled on Part 744.6 would make sense in this context. However, because of the unduly short comment deadline, the Coalition has not yet made a final determination about whether it would fully support this type of construct. Of course, the Coalition would also have to judge any such proposal on its detailed language, so we look forward to a subsequent proposed rule from BIS that takes a more thoughtful approach.

B. “Band aids” That May Patch a Hole But Will Not Fix the Fundamental Problem With the Proposed Rule

The Coalition hopes that BIS will not delay productive conversations on this topic by trying to fix its broken rule. Malicious cyber-attacks are a clear and present danger to our national security and economic competitiveness, and the scarce resources behind this effort should not be spent focusing on an approach that will not work. Nonetheless, to demonstrate the efforts the Coalition has undertaken to think about whether it would be possible to fix the current proposed rule, we lay out some of those ideas below. These proposals would help make the proposed rule somewhat less harmful, but they will not make it any more effective.

1. License Exception for Legitimate Security End-Uses

It may be possible to craft a broad license exception for legitimate cybersecurity end-uses, which could significantly decrease the negative side-effects of the proposed rule. Of course, such a broad license exception would not make the controls any more effective in targeting the malicious conduct for which they were ostensibly designed—the only way the Coalition is aware of to accomplish that goal would be to reshape the prohibition itself around intent and end-use rather than sticking with a strict liability item/destination framework. But it still may be worth thinking about how a broad license exception like this would work.

There are already examples in the EAR of broad license exceptions based on end-use. For example, License Exception CIV authorizes exports and reexports of certain items on the CCL that are controlled for national security (NS) reasons only and destined to civil end-users for civil end-uses in certain listed countries.⁸⁴ If a similar license exception could be created to

⁸³ Section 744.6(a)(1)(ii) and (a)(2)(i) and (ii).

⁸⁴ Section 740.5.

allow legitimate cybersecurity companies to continue to operate unrestricted by a licensing burden (including deemed exports), such a proposal may satisfy many of the Coalition’s concerns. Unlike License Exception CIV, however, such a provision could not contain significant geographical limitations, given the global nature of the cybersecurity world.

A broad license exception of this type could be based on security or defense, data protection, or similar end-uses. For example, it could include language such as “software designed to add security or benign functionality beyond the original intent of the designer of the system or software that it enhances.” Another possibility would be a license exception for end-uses or added functionality with the knowledge and consent of the authorized user, system administrator, or network owner. In either case, like License Exception CIV, such a provision could impose liability if the person “knows” the item is intended for malicious end-uses or end-users. That would look somewhat similar to the Part 744.6 controls discussed above, but there would still be a need to create an underlying prohibition that makes sense, which is why we believe that removing these systems, software, and technology from the construct of the CCL, and instead working this control regime into Part 744.6 in the first place, would be the best approach.

Any attempt to make such a license exception too specific would probably not be workable. For instance, license exceptions for penetration testing and red teaming (where a group of security professionals accesses an organization’s system in ways similar to malicious actors to test its defenses) would again run into the problem of becoming almost immediately obsolete. It is simply not feasible to try to draw up specific exceptions for products and services available today. Even a fully inclusive list of all products and services available today cannot account for cybersecurity defenses that have not yet been invented and cannot today be contemplated. As attacks evolve so must defenses, and such a limited approach would undoubtedly hamper innovation in new defensive capabilities that are unknown today but may be critical tomorrow.

2. License Exception Based on End-User Statements

Another potential model for a broad license exception could be one requiring certain assurances from the end-user. For example, License Exception TSR permits exports and reexports of certain technology and software controlled for NS reasons only, but again only when destined to certain countries.⁸⁵ License Exception TSR requires a written assurance in advance from the consignee or importer that it will not, without BIS authorization, engage in certain prohibited exports or reexports of the technology or software. This model could be applied in the cybersecurity context by requiring an assurance regarding unauthorized re-transfers, end-uses without the knowledge and consent of the authorized user, system administrator, or network owner, or limited end-use only for the purpose of protecting the end-user’s own system. However, again, any such license exception would not be workable if it contained significant geographical limitations. And an even more significant limitation on the effectiveness of such a requirement would be the reluctance of non-U.S. researchers—often working as volunteers—to sign such a limitation that is presented to them by a party with whom they may not have a contractual or other formal relationship.

⁸⁵ Part 740.6.

3. License Exception for Transfers Among Parties to a Contract or Non-Disclosure Agreement

Another idea would be to create a license exception that would permit transfers to customers or third parties with which a U.S. company has a contractual relationship, non-disclosure agreement (“NDA”), or information sharing agreement. That would address a sizeable portion of the cybersecurity business, but it would cut off a critical population of third-party researchers and collaborators who will only work with U.S. companies on an informal basis. Because many of those individuals will never be convinced to sign a piece of paper, this type of solution will never allow the U.S. cybersecurity industry to stay on the cutting-edge. If there are other ways to address exchanges with those informal business partners, e.g. some sort of basic reporting requirement, it is conceivable that this type of provision could constitute a partial solution, but, at the very least, it would have to be in conjunction with large carve-outs for internal company operations (e.g. deemed exports and intracompany transfers, discussed below).

4. License Exception for Activities Compliant with Software Terms and Conditions

Some outside the Coalition have raised the idea of creating a carve-out for activities conducted within the scope of software license terms and conditions. The idea would be, for example, that it should not be prohibited for a cybersecurity company to probe or add functionality to an off-the-shelf program like Microsoft Word in a way that does not violate the terms and conditions imposed by Microsoft on Word users or if allowed by the authorized user, system administrator, or network owner. In contrast, those terms and conditions may in theory prohibit the type of activities that malicious actors would engage in, so those activities would remain prohibited. However, such a solution is not likely to be workable in most instances, because software terms and conditions generally do not contain prohibitions that would be relevant in this context. Instead, they tend to simply disclaim any warranties based on misuse or alteration of the product, which would not be helpful in distinguishing malicious activity from legitimate defensive activity. And, even where they are restrictive enough to prohibit malicious activity, they may do so in a way that also prohibits benign software innovation and addition of functionality that the authorized user, system administrator, or network owner desires. Therefore, the Coalition does not view this type of proposal as being particularly promising, but it may be worth exploring in more detail at a later date.

5. Carve-Outs for Deemed Exports and Intracompany Transfers

In conjunction with some sort of broad carve-out for customer and third-party transfers like the one discussed in Section VII.B.3, above, a broad permissive provision related to deemed exports and intracompany transfers would relieve a significant portion of the Coalition’s concerns regarding the proposed rule.

6. License Exception ENC Framework

One example from the existing encryption controls that could provide a basic theoretical framework is License Exception ENC, which authorizes exports and reexports of certain encryption items to certain end-users in certain countries for certain end-uses without the submission of encryption registrations, classification requests, self-classification reports or sales

reports.⁸⁶ License Exception ENC is far more restrictive than any viable counterpart could be for cybersecurity items. The geographical restrictions in particular would be problematic, but any item type, end-user or end-use limitations would also have to be carefully crafted to account for the nuances of how the cybersecurity sector works. Furthermore, any registration or reporting requirement would have to take account of the constantly-changing nature of cybersecurity technology, and could not, for instance, require re-submission with each change in functionality. Nor could it mandate an unduly burdensome level of disclosure, particularly regarding certain sensitive third-party relationships and current vulnerabilities. Importantly, any waiting period (e.g. like the 30-day waiting period under ENC) would likely make such a provision unworkable. Overall, while License Exception ENC may provide a basic theoretical model for how a cybersecurity provision may work at a macro level, the details would have to be significantly adapted to the realities of this industry.

It is also important to note that this type of hands-on regulatory framework may not be feasible for smaller companies, researchers and independent operators—a vital part of the U.S. cybersecurity community—who would not have the resources to comply. Creating barriers to entry of this kind generally leads to stagnation of the market and hinders innovation.

7. Note 4 to Category 5, Part 2

Another possible model for cybersecurity items is the decontrol available for encryption items in Note 4 to Category 5, Part 2. Note 4 states that Category 5, Part 2 does not apply to items using “cryptography” that do not have certain “primary functions” (such as information security; a computer; sending, receiving, or storing information except in certain circumstances; or networking), as well as certain other requirements. A similar test related to “primary function” could be proposed for cybersecurity items (for example, “intrusion software, whose primary function is the protection of data or systems or that is intended to be used with a network owner’s or system administrator’s knowledge and consent”).

8. Less Tightly Controlled ECCNs

Another potential model could be the less tightly controlled ECCNs covering certain encryption items.⁸⁷ Encryption items under these ECCNs are only controlled for anti-terrorism (AT) reasons and therefore can be exported without a license to most destinations. A cybersecurity analog could include items like mass market products, benign or authorized end-uses, etc.

⁸⁶ Part 740.17.

⁸⁷ For example, encryption items that fall under “5x992” ECCNs include those with weak encryption (below 56 bits for symmetric algorithms and below 512 bits for asymmetric algorithms); limited encryption functionality (authentication, access controls, digital signatures, financial data, “fixed” compression or encoding, etc.); unused or disabled encryption functionality; and mass market items (publicly sold without restriction, where the cryptographic functionality cannot be easily changed by the user and it is designed for installation without support).

VIII. CONCLUSION

Given all of the fundamental flaws and unworkable provisions in the proposed rule identified and discussed above, BIS should go back to the drawing board and begin again to consider how to control malicious cyber items from a clean slate. As described in detail above, the current proposed rule is fundamentally flawed and should not serve as the starting-point for any future proposed rule. To implement the current proposed rule would be devastating to U.S. cybersecurity. We hope that BIS will view this first proposed rule and the comments received in response as a valuable learning exercise that demonstrated how damaging and ineffective the proposed rule would be, as well as a framework from which to approach future Wassenaar discussions.

Because critical defensive products and methods are technically indistinguishable from malicious tools, because of the global nature of the workforce, and because these technologies are changing so rapidly, BIS should not continue to pursue controls that are based on the classification of the item (i.e. its functional characteristics) and the country of destination. Any future control regimes that are proposed should focus on the intended end-use, since that is the only way of separating defensive from offensive tools. Such a control regime would also have to take account of the entire cybersecurity community—including established companies, start-ups, academics, and independent researchers—because fencing off any part of this community would have devastating effects on innovation and on U.S. companies' ability to stay ahead of the global threat environment. Furthermore, any workable controls cannot contain significant geographic restrictions, because some of the most risky countries from a threat perspective are also the most critical places for U.S. companies to be able to protect themselves adequately. Finally, any cybersecurity controls must not impose any requirements that involve waiting periods for critical activity, because this sector operates in seconds and minutes, not weeks and months.

The Coalition would be pleased to offer whatever additional support it can to help the U.S. government craft a regulatory regime that will work. We hope that some of the ideas we have raised in Section VII.A will be a useful starting point for a new proposed rule, but, again, we will need more time to consider how any controls modeled on Part 744.6 or other proposed modifications or approaches would work in practice in our industry before we can express any definitive opinion. It is important that we work together to get this right, for the sake of our collective national security and future economic competitiveness, and to find a way of countering the very real threats that exist in a way that will be effective. If you have any questions please do not hesitate to contact Meredith Rathbone (202-429-6437; mrathbone@steptoe.com), Stewart Baker (202-429-6402; sbaker@steptoe.com) or Alan Cohn (202-429-6283; acohn@steptoe.com).

Respectfully submitted,



Meredith Rathbone
Stewart A. Baker
Alan Cohn
STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, NW
(202) 429-3000
mrathbone@steptoe.com
sbaker@steptoe.com
acohn@steptoe.com

On behalf of the following members and supporters of the Coalition for Responsible Cybersecurity:

IONIC SECURITY INC.
Adam Ghetti, CTO
Robert Ball, Chief Legal Counsel
Ryan Speers, Director Applied Research

SYMANTEC CORPORATION
Cheri F. McGuire, Vice President, Global Government Affairs & Cybersecurity Policy

FIREEYE, INC.
Shane McGee, Chief Privacy Officer
Orlie Yaniv, Director, Government Affairs and Policy

SYNACK, INC.
Mark Kuhr, CTO

TRAIL OF BITS, INC.
Dan Guido, Co-Founder and CEO

PUBLIC SUBMISSION

As of: 7/29/15 6:36 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-eg2y
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0261

Electronic Frontier Foundation Nate cardozo 7-29

Submitter Information

General Comment

See attached

Attachments

Electronic Frontier Foundation Nate cardozo 7-29



ELECTRONIC FRONTIER FOUNDATION

eff.org

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th St. and Pennsylvania Ave. NW.
Washington, DC 20230

VIA Email: publiccomments@bis.doc.gov

RE: Comments of the Electronic Frontier Foundation on the Wassenaar Arrangement 2013
Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49

To Whom it May Concern:

The Electronic Frontier Foundation (EFF) submits the following comments to the Bureau of Industry and Security (BIS) in response to the Proposed Rule and Request for Comments on the Wassenaar Arrangement (WA) 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, RIN 0694-AG49, dated May 20 2015 (Proposed Rule). In addition to these comments, EFF joins in full the comments submitted by the group of civil society organizations consisting of Access, Center for Democracy and Technology, Collin Anderson, EFF, Human Rights Watch, and New America's Open Technology Institute (Joint Comments). We submit these brief comments to supplement and expand on our more complete joint civil society submission.

We urge BIS to revise the Proposed Rule and open another public Request for Comments on the revision. As part of that process, we urge BIS to take what it learns as part of this rulemaking to the greater international export control community in December 2015 at the next annual meeting of the WA members, and work with them to improve the text of the WA control lists directly.

BIS is familiar with the Wassenaar Arrangement and the 2013 additions to the WA control lists so we will not summarize them or their history here. Similarly, because EFF is a legal organization and not a software vendor, we will not focus on specific products here, except when necessary. We understand that several knowledgeable companies and trade organizations will be submitting comments to this Proposed Rule and we trust them to give specific examples of how the Proposed Rule will impact their businesses directly. These comments are instead intended to give an overview of what we think some major issues with the Proposed Rule are, and some ways in which BIS might address them.

These comments are limited to the addition of intrusion software controls in ECCN 4A005 and related amendments to ECCN 4D001, ECCN 4E001, and § 740.13; we do not address the Proposed Rule as it applies to ECCN 5A001.j regarding Internet Protocol (IP) Network Communications Surveillance Systems.

1. About the Electronic Frontier Foundation

EFF is a nonprofit, member-supported civil liberties organization working to protect privacy and free expression in technology, law, policy, and standards in the information society. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With

over 21,000 dues-paying members and over 284,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

EFF has been a leading voice defending the rights of security researchers since the 1990s when we represented Professor Daniel J. Bernstein in his successful challenge to the inclusion of open source cryptography in the International Traffic in Arms Regulations (ITAR). We believe that the Proposed Rule is too vague to be feasible, technically flawed, and almost certainly unconstitutional.

2. Specific Concerns and Recommendations

- Eliminate Encryption Items from the EAR

Strong cryptography is a necessary and daily part of our lives in the digital era. The freedom to use encryption technology is often a prerequisite for everything from online commerce to the exercise of the rights of privacy and expression, that it can no longer be rationally thought of as a dual-use technology. As it notes in the preamble, many of the technologies the Proposed Rule would control “are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality” and therefore the rule would add little additional burden. Much of the work of the Proposed Rule seems to hinge on that assumption and much of BIS’ response to questions about the scope of the Proposed Rule refer to the fact that intrusion software is often already controlled if it contains encryption or cryptanalytic

functionality. However, cryptography is a core component of everything from web browsers,¹ to mobile phones,² to music players³ and as such, does not reasonably belong in the EAR.

Both individuals and government agencies rely on strong encryption in their daily activities. Moreover, human rights activists, journalists, refugees, bloggers, and whistleblowers rely on strong encryption technologies to protect their communications, the names and location of their sources and/or witnesses, etc. Even the relatively hands-off control of encryption in the EAR impacts freedom of expression in two ways. First and foremost, it makes it harder for small developers to publish their work. Second, any attempt to restrict the distribution of encryption technologies that did not follow the EAR's process would impact the rights of software creators to express their viewpoint through code. Furthermore, many security researchers provide open-source encryption software and disclose algorithms as an integral part of examining the encryption technology for flaws and weakness. This means that the encryption technology purportedly controlled by the EAR is already freely available throughout the world. It is time for the EAR to be updated to reflect the fact that encryption is a civilian technology that is critical to protecting our democracy, our right to free expression, and our security.

The encryption controls should be removed from Category 5 part 2 of the EAR as part of any revision to the Proposed Rule. The controls on Encryption Items function only to impose a bureaucratic headache on American businesses and developers without any benefit to commerce or national security.

¹ <http://research.google.com/pubs/SecurityCryptographyandPrivacy.html>

² https://www.apple.com/business/docs/iOS_Security_Guide.pdf

³ https://sonos.custhelp.com/app/answers/detail/a_id/2638/~~/sonos-wifi-setup

- BIS Should Revise the Proposed Rule and Open a New Request for Comments

EFF is confident that BIS will revise the Proposed Rule in response to the comments it receives in this rulemaking. However, in order to avoid the technical ambiguity that plagues this Proposed Rule, the revision process must be iterative and collaborative. Even though it will unavoidably introduce delay into the process, BIS should issue a revised Proposed Rule and reopen a public Request for Comments on the revisions to the Proposed Rule after consulting with industry, academia, and civil society.

Further, BIS cannot and does not operate in a vacuum. Much of the technically problematic language from the Proposed Rule (e.g., defining “intrusion software” as software that performs a “modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions”) comes directly from the WA. As such, we urge BIS to work within the WA at the December 2015 annual meeting to ensure that changes to the definitions are integrated upstream into the WA control lists themselves. We urge BIS to wait until after that process is complete before issuing a revised Proposed Rule and Request for Comments.

- BIS Should Clarify What it Intends to Control

For years, there’s been ample evidence that authoritarian governments around the world are relying on the technology of U.S. and European companies to facilitate abuse of human rights, with a wealth of recent evidence in the Arab Spring and China. But in the Preamble to the Proposed Rule, BIS does not actually state its goal for this rule, but instead parrots the control lists’ definitions.

That lack of clarity has left the public having to guess what BIS' aims are and which types of technologies BIS intends to regulate. Some of that confusion is inherent in the WA language itself, but much of it comes from a lack of clear limiting statement from BIS. And as BIS has seen over the last two months, there has been an overwhelming need for clarification of the rules.⁴

As it revises the Proposed Rule, we urge BIS to also revise the Preamble to present a clear statement on the *intended* scope of the regulation. Simply repeating the technical language from the control lists caused more confusion than it resolved. Does BIS intend to control only those systems that are specially designed for use by governments? If so, BIS should clearly so state.

From the perspective of academics, security researchers, and open-source developers, it would be better to be faced with a clearly-worded, clearly-defined rule that the community did not necessarily agree with, than a difficult to understand rule that seemed to implement policies that the community would support, if only it could only understand what the rule meant. To give a specific example, in FAQ #4,⁵ BIS stated that the Proposed Rule would control “information ‘required for’ developing, testing, refining, and evaluating ‘intrusion software’, in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information.” It is clear to EFF that BIS does not intend to control penetration testing frameworks or debuggers, but from the answer to the FAQ above, that intent is not effectively conveyed.

⁴ See, e.g., the fact that a 32-question FAQ was necessary.
<https://www.bis.doc.gov/index.php/policy-guidance/faqs#subcat200>

⁵ *Id.*

The vagueness of the WA control lists has real world chilling effects on fundamental academic research. Take for example the dissertation of a student at the University of Northumbria named Grant Wilcox.⁶ EFF does not believe that censorship of Mr. Wilcox's paper required by the WA control lists. However, the fact of the matter is that Mr. Wilcox's university ethics board did censor the dissertation, believing it to be possibly within the WA definitions. This instance is only one recent and particularly clear example among many of the unintended chilling effects of vaguely worded regulation. From an EFF perspective, examples such as the needless censorship of Mr. Wilcox's dissertation strongly caution against proceeding with an implementation of the WA in the United States without first clarifying the scope of what exactly the rules are intended to control.

- Potential Constitutional Problems with the Proposed Rule

EFF understands that BIS is seeking information about the effect of the Proposed Rule specifically as applied to industry and is not inviting legal arguments. However, the nature of EFF compels us to point out two potential constitutional problems with the Proposed Rule that would likely cause a court to invalidate the rule if it went into effect as currently drafted, or at best tie it up in litigation for years before it went into effect.

First, the Proposed Rule would act as an unconstitutional prior restraint on speech in violation of the First Amendment. In 1999, a U.S. Court of Appeal agreed with EFF that a broad range of individual rights were implicated by government controls on the discussion of source code:

[W]e note that the government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment

⁶ <http://tekwizz123.blogspot.com/2015/07/final-year-dissertation-paper-release.html>

rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic “fingerprints” behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption’s bounty. Viewed from this perspective, the government’s efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, see *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 115 S.Ct. 1511, 1524, 131 L.Ed.2d 426 (1995), the right against compelled speech, see *Wooley v. Maynard*, 430 U.S. 705, 714, 97 S.Ct. 1428, 51 L.Ed.2d 752 (1977), and the right to informational privacy, see *Whalen v. Roe*, 429 U.S. 589, 599-600, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977).

Bernstein v. United States Dept. of Justice, 176 F.3d 1132, 1145-46 (9th Cir. 1999). While the Ninth Circuit in *Bernstein* was discussing the encryption rather than the cybersecurity items controlled by the Proposed Rule, much of the reasoning is similarly applicable. By failing to adequately consider the technology, information, and tools necessary for industry professionals to protect the digital security we all depend on,⁷ the Proposed Rule implicates more than just the rights of security software vendors. Any attempt to slow or stop the advancement of the state of the art of computer security through control under the EAR will be subject to the highest level of constitutional scrutiny. A narrowly-cabined rule, one limited to controls of end uses or end users,

⁷ See e.g., Comment of Cisco Systems, Inc.
https://blogs.cisco.com/wp-content/uploads/Cisco_Wassenaar_Final_07202015.pdf

as we recommend in the Joint Comments would be much more likely to stand up if challenged in court.

Second, if regulations that carry criminal penalties (as the EAR does, *see* 15 C.F.R. § 764.3(b)), those regulations “are impermissibly vague [if] they fail to give notice of the conduct they regulate and have a chilling effect on speech.”⁸ Only if the definition of prohibited conduct as well as “the exemptions from this definition are clear to a person of ordinary intelligence” may a criminal penalty pass constitutional muster.⁹ As worded, the Proposed Rule and its exemptions are not clear to a person of ordinary intelligence. BIS’ own FAQ in response to the Proposed Rule is ample demonstration that persons of much greater than ordinary intelligence are confused by the Proposed Rule. Therefore unless BIS revises the Proposed Rule to the point where it is “clear to a person of ordinary intelligence”—not an industry insider, an export control lawyer, or the rare software developer versed in parsing statutory language—a court would be likely to strike down the rule as unconstitutionally vague.

3. Conclusion

EFF respectfully urges BIS to carefully consider the quality and quantity of the comments it receives in opposition to the current Proposed Rule. In addition to the comments submitted by the group of civil society organizations consisting of Access, Center for Democracy and Technology, Collin Anderson, EFF, Human Rights Watch, and New America’s Open Technology Institute, we urge BIS to (1) eliminate all controls on cryptography from the EAR before proceeding with implementing the Wassenaar Arrangement 2013 Plenary Agreement, (2)

⁸ *Bernstein v. US Dept. of State*, 922 F. Supp. 1426, 1439 (N.D. Cal. 1996).

⁹ *Id.*

revise the Proposed Rule and reopen a second public comment period, and (3) carefully consider the Due Process and First Amendment implications of any vaguely-worded prior restraint of the dissemination of knowledge.

Sincerely

A handwritten signature in black ink, appearing to read "Nate Cardozo". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Nate Cardozo
Staff Attorney
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94611

PUBLIC SUBMISSION

As of: 7/29/15 6:38 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-4g8t
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0262

Electric Power Research Institute York Huang 7-29

Submitter Information

General Comment

See attached

Attachments

Electric Power Research Institute York Huang 7-29

July 20, 2015

Via email to publiccomments@bis.doc.gov

Regulatory Policy Division
Bureau of Industry and Security
Room 2099 B
U.S. Department of Commerce
14th St. and Pennsylvania Ave., N.W.
Washington, D.C. 20230

Re: RIN 0694-AG49 - BIS-2015-0011: Comments to Wassenaar Arrangement 2013 Plenary
Agreements Implementation: Intrusion and Surveillance Items Proposed Rule

Dear Sir or Madam:

The Electric Power Research Institute, Inc. (“EPRI”) respectfully submits comments to the Commerce Department’s Bureau of Industry and Security (“BIS”) on the proposed rule on intrusion and surveillance items in implementation of the Wassenaar Arrangement. EPRI appreciates the opportunity to provide these comments.

EPRI is a nonprofit corporation organized under the laws of the District of Columbia Nonprofit Corporation Act and recognized as a tax exempt organization under Section 501(c)(3) of the U.S. Internal Revenue Code of 1986, as amended, and acts in furtherance of its public benefit mission. EPRI was established in 1972 and has principal offices and laboratories located in Palo Alto, CA; Charlotte, NC; Knoxville, TN; and Lenox, MA. EPRI conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, health, safety and the environment. EPRI also provides technology, policy and economic analyses to inform long-range research and development planning, as well as supports research in emerging technologies. EPRI has had established research efforts on cybersecurity and the utility industry since 2002. Its cybersecurity program focuses on addressing the emerging threats to the electric sector through collaborative research on cybersecurity technologies, standards, and business processes.

It is important in the U.S. national interest and that of EPRI’s members and society generally, that tools are available to counter the constantly changing world of cyber-attacks. Any toolkit must include not only “defensive” tools to protect cyber networks, but also “offensive” tools for assessing the quality of “defensive” tools. In fact, EPRI’s research includes both “defensive” and “offensive” tools, the latter of which EPRI believes must be readily available for

Together . . . Shaping the Future of Electricity

collaborative research purposes. EPRI is concerned that the time and resource implications of the strict licensing requirements proposed to be imposed on the new Export Control Classification Numbers (ECCNs) could curb companies' efforts to protect their cyber networks and result in less certainty about the quality of available protection mechanisms. If the result of the regulations is that "offensive" tools will not be as available for research and for companies' efforts to evaluate the effectiveness of defensive measures, then the rules have the potential to make life more difficult for "white hat" hackers dedicated to thwarting intrusive attacks.

EPRI understands that BIS is seeking comments in particular with respect to the impact the proposed rules would have on increasing licensing applications. In response, EPRI's comments aim to offer practical suggestions with a focus on how regulatory mechanisms that already exist within the Export Administration Regulations (EAR) may be adapted or otherwise made available with respect to cybersecurity items. EPRI believes doing so would lessen the burden on exporters legitimately involved in protecting cyber networks while still accomplishing BIS's broader objectives and fulfilling U.S. commitments under the Wassenaar Arrangement. Below we identify and discuss each of these suggestions, some of which are adopted from BIS's rules and practice concerning encryption items, which we believe are particularly useful given that the export of many of the proposed cybersecurity items has already been controlled for that purpose.

- Bulk Export License Authorization
- Expanding List of Exempt Countries
- Foreign Offices and Subsidiaries
- Deemed Exports and Reexports
- License Exception for Research
- Grandfathering

1. Bulk Export License Authorization

Based on EPRI's many years of experience in and knowledge of the cybersecurity industry relating to the energy sector, EPRI anticipates that the new ECCNs would significantly increase the number of export license applications, especially considering that cybersecurity is relevant for all sectors that utilize electronic networks. For EPRI, this could mean that each piece of relevant software or hardware or each instance of technical consultation that involves non-U.S. customers, employees and contractors, could trigger a controlled export for which EPRI would first need to obtain an export license.

In view of the added burden this would place both on exporters, including researchers, as well as on the administrative resources of BIS, EPRI suggests that a form of bulk export license authorization be made available for the new ECCNs under certain circumstances. For example, under section 742.15 (a)(2) of the encryption controls, BIS permits exporters to apply for an Encryption Licensing Arrangement, which authorizes the export of unlimited quantities of such items to specified end-users and previously also authorized such transactions with foreign commercial partners. EPRI believes adoption of such an export license authorization mechanism for cybersecurity items would enable the use of one application to apply for approval on more of a program basis.

2. Expanding List of Exempt Countries

BIS has indicated that the cybersecurity rules have been proposed to fulfill U.S. commitments under the Wassenaar Arrangement yet only Canada would be exempt from the licensing requirements. EPRI's current international customers and contractors in the area of cybersecurity are largely based in countries which (like the U.S. and Canada) also are Participating States under the Wassenaar Arrangement, including within the European Union (France, Germany, Ireland, Poland, Spain, and the United Kingdom), as well as other industrialized countries in Asia such as Japan and South Korea. BIS may consider expanding the list of exempt countries to those in the Wassenaar Arrangement.

In the alternative, following the example of the encryption rules, BIS could take steps to facilitate cybersecurity exports to specified countries under certain circumstances. For example, under section 740.17 (a)(1) of the EAR, within License Exception ENC, exports of encryption items to companies headquartered in a Supplement No. 3 country are exempt from needing prior authorization, if the export is for internal development or production of new products. Even if BIS also required a pre-export notification or post-export report in order to be informed of the identity of the recipients, adopting a similar narrowly-tailored mechanism within the cybersecurity rules could facilitate the important endeavor of enabling business partners in like-minded states to legitimately collaborate on developing tools to protect cyber networks.

3. Foreign Offices and Subsidiaries

BIS indicates that export license applications for cybersecurity items destined to a U.S. company or subsidiary in other than Country Group D:1 or E:1 are proposed to be reviewed favorably. However, EPRI submits that BIS can treat exports under such circumstances even more favorably and that it has already been demonstrated this can be done effectively consistent with U.S. policy objectives. Specifically, section 740.17 (a)(2) of the EAR authorizes the export of encryption items without a license or other authorization to any "U.S. subsidiary," and the EAR contains a specific definition in Part 772.1 for this purpose. Even though various aspects of the encryption rules have been continuously revised over the last 15 years, this provision has remained unchanged since 2000, indicating the exemption has been effective.

4. Deemed Exports and Reexports

BIS indicates in the proposed rule that implementation of these Wassenaar Arrangement (“WA”) changes “ensures U.S. companies have a level playing field with their competitors in other WA member states.” However, the EAR’s provisions on deemed exports and reexports will actually prevent that as EPRI understands this concept does not exist in most if not all other export control regimes. This means that U.S. companies in the cybersecurity space will actually be placed at a disadvantage compared to their WA counterparts using non-U.S. technology.

To try to mitigate this within the context of the rules, EPRI proposes that BIS adopt for cybersecurity a version of the approach undertaken in the encryption rules. Specifically, section 734.2 (b)(9)(i)(B) of the EAR exempts encryption source code from being considered a deemed export unless transferred to a foreign government. Also, as part of the provision discussed above regarding U.S. subsidiaries, section 740.17 (a)(2) of the EAR generally authorizes within License Exception ENC deemed exports of encryption technology, e.g., to foreign national employees and individual contractors of a U.S. company or its subsidiaries, if the items are for internal company use, including development and production of new products. Adopting these approaches for cybersecurity will better ensure U.S. companies can continue to effectively compete to attract the world’s best technical talent.

5. License Exception for Research

EPRI suggests that BIS consider whether a research exception to the general export licensing requirement could be carved out for public benefit research conducted by U.S. nonprofit entities such as EPRI. This idea is inspired by the February 2015 Department of Energy (DOE) final rulemaking on “Assistance to Foreign Atomic Energy Activities,” which codifies DOE’s export controls under 10 C.F.R. Part 810. After a rulemaking and comment period that lasted over three years and resulted in the most extensive changes ever made to these rules, DOE determined to allow certain research activities with respect to Mexico in conjunction with International Atomic Energy Agency (IAEA)-related research scopes, to be exempt from new licensing requirements.

6. Grandfathering

To allow completion of existing cybersecurity related research projects and minimize potential breaches of contractual obligations which would be detrimental to EPRI and other U.S. companies, EPRI suggests that a grandfathering clause be included in the implementation of the final rules. Specifically, such a clause could include a grace period or phase-in period within which companies could continue existing activities as long as they submitted export license applications within a reasonable period of time thereafter.

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
July 20, 2015
Page 5

Conclusion

EPRI trusts that these comments may provide BIS with practical ideas for fine-tuning the proposed new rule. EPRI thanks BIS for its review and consideration. Should BIS need any clarification or further information regarding any of the suggestions above, please do not hesitate to contact the undersigned.

Best regards,

A handwritten signature in blue ink, appearing to read "Salvador A. Casente, Jr.", with a long horizontal flourish extending to the right.

SC150720.01

c: Michael W. Howard

PUBLIC SUBMISSION

As of: 7/29/15 6:39 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-xx8u
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0263

Data Security Council of India (DSCI) Nandkumar Saravade 7-29

Submitter Information

General Comment

See attached

Attachments

Data Security Council of India (DSCI) Nandkumar Saravade 7-29

NASSCOM-DSCI Comments on BIS proposal to include cyber security items in the export control regime

On behalf of NASSCOM (National Association of Software and Services Companies) and DSCI (Data Security Council of India) and our member organizations, we write to express our deep concern with the proposed rule by the Commerce Department, Bureau of Industry and Security (“BIS”), US Federal Government, in the Federal Register on May 20, 2015 (the “Proposed Rule”). Wassenaar Agreement is recognized, among others, for restriction on export of encryption technologies. The current proposal discusses incorporation of intrusion and surveillance software into the scope of the Agreement and mentions reviewing ‘cyber security items’ explicitly. Use of such items is commercially prevalent and widely deployed in both public and private sector organizations across the world. The new rules, although well intentioned in curbing cyber weapon and espionage tools used illegally and for protecting national interests, may well end up hindering the growth of technology development and economic activity in the cyber security domain and could, in the long run, weaken the global cyber security posture. Following are some of the pointers that we would like to highlight as potential problems with the proposed amendments to the existing rules:

- Overly broad definition of “intrusion software” (software that is capable of extracting or modifying data or modifying the standard execution path of software in order to allow the execution of externally provided instructions) coupled with the rules and explanation provided by BIS in FAQ#1 (“the Category 4 control entries would control the command and delivery platforms for generating, operating, delivering, and communicating with ‘intrusion software’”. It would also control the technology for developing ‘intrusion software’”) and FAQ #2 on its website (The rule would control the export of hardware and software delivery tools, as well as the export of technical data for developing exploits (“intrusion software”)), could cover almost all categories of ICT software and products.

Security defense, which is critically dependent on vulnerability research and intrusion detection, would be hampered because of the proposed restrictions. Sectors, public and private, would be constrained to use the solutions that are built on inadequate vulnerability research and intrusion detection technique. The security technology corporations of the US, who are dominant in the Indian security market may not be able to export the final products involving these technologies for use in India, which will cause disruption in security ICT supply chain and trade flows.

- The proposed rule could also create significant hindrances in technology transfer and sharing of intellectual property rights in case of mergers and acquisitions by companies belonging to

countries that are not signatory to the Wassenaar Agreement. Many companies in the US have their Research and Development (R&D) centers in countries like India. The rules have the potential to hamper the prospects of US-headquartered companies leveraging expertise and skilled manpower provided by India, as there is no license exception for intra-company transfers or internal use by a company headquartered in the United States under the proposed rule. In the age of hyper-specialization and globalization, this could prove counter-productive.

- With emergence of new technology and platforms in the security domain, vulnerability discovery and exploitation are on constant rise. The FAQs state that public disclosure provides an exemption: “..export controls do not apply to any technology or software that is “published” or otherwise made publicly available.”

However, not all parts of vulnerability information sent to a vendor are necessarily publicly disclosed when they are discovered. Must all the data provided, including proof-of-concept code, be published in order for the exemption to apply? The current rules could have a stifling impact on vulnerability disclosure, and could thus dampen overall security regime.

Recent innovations in discovery of vulnerabilities through the bug bounty competition and hackathons will be affected adversely. Such programs are extremely useful to draw the young fresh talent into the security domain and build capacity. BIS draft, if passed in current form, could even shrink the security talent pool, which is already in short supply globally.

- The rules could also hamper product development, which is dependent on vulnerability research and security use cases. It could hamper prospects of developing enterprise grade products by companies located in countries such as India. Capabilities and functionalities from different sources and countries are integrated to develop products. Restrictions imposed by such rules would seriously hamper supply chain and many economies will be deprived of such possibilities. Because of low production, the overall security regime might suffer with lower availability of mature security products.
- The proposal adds additional restrictions on development, production and use of equipment, probably with an intent of establish control over the life cycle of the equipment. This would be seriously hamper the supply chain involving these technologies and inhibit development and production out of the US using any component listed here.

- ECCN 4D001 talks about control of software, specially designed for intrusion or surveillance. Restriction of this nature is an attempt to retain the control of surveillance and intrusion software in the country.
- Export Control Classification Numbers (ECCN) 4A005 and 4D004 state that no license exception would be available to these items, expect some provision. These ECCNs are proposed to be controlled for national security (NS) and regional stability (RS) and anti-terrorism (AT) reasons to all destinations except Canada.

This clearly indicates that authorities responsible for NS, RS and AT would have a lot of empowerment to intervene into the export of technologies that are useful in the commercial space. With Cyber Security introduced as a category, more such intervention would happen in the future.

- Although cyber security policy controlled under National Security (NS) and Anti- Terrorism (AT) will not be revised, there is a proposal to revise items controlled by Regional Stability (RS). It proposes to consider case of government and end users in Australia, New Zealand, or the UK favorably on case-to-case basis as they have partnered with the US on cyber security policy and issues. While certain countries would get benefit of the policy change, countries out of this orbit, like India would be at significant disadvantage.
- The new addition to rule would restrict exception to license of cyber security items involving encryption. The new addition also proposes to add a requirement to submit specific technical information in support of export, re-export, or transfer cyber security items. These additions are bound to create problems with respect to use of and development of the technologies listed under cyber security. Secondly, transfer of these technologies would be subjected to these requirements.
- Rule proposes that upon request from BIS, the applicant must include a copy of the section of source code and other software (libraries and header files) that implement or invoke the controlled cyber security functionality. Such requirements can impact commercial viability of products used in critical infrastructure in other countries with possible suspect that it could lead to surveillance activities and vulnerability exploitation.

- Bringing protocols such as ICAP that are used to decrypt SSL traffic for identifying malicious traffic, under export control regime, could restrict export of solutions incorporating such protocol.
- The rules based on requirement to obtain export license for selling products based on the nationality of individuals working on the technology and product could potentially act as the biggest barrier and be detrimental in technology development as organizations across the globe engage and source experts from all over the world to develop enterprise grade technology platforms and products.
- Under the proposed rules and clarification thus provided in FAQ #17, all exports of specified systems, equipment, components or software that would generate, operate, deliver or communicate with "intrusion software" would require an export license.
- In the Internet age, as we are beginning to leverage benefits of Internet of Things (IoT), the technology components across all layers are integrated. All devices over the Internet and networks (smartphones, laptops, tablets, applications, software, servers, etc.) speak to each other and generate and collect data and information for meaningful analytics and intelligence. Above rules have the scope and ambit to include all ICT devices, which could lead to increased restrictions on transfer of ICT devices if covered under the export control regime.
- Inclusion of Penetration Testing software and products and its broad definition potentially covering legitimate software and tools used by organizations for enhancing their security posture, as has also been acknowledged in the FAQs, could lead to curb in usage because of it being under the ambit of export control.
- Companies in US and those signatory to Wassenaar Agreement are likely to err on the safer side and stop employing people and exchanging vulnerability data in order to demonstrate compliance to the proposed rules.

The proposed regulations may put many legitimate technology and services companies out of business due to excessive regulatory controls such as license applications burdens, compliance requirements, delays in approvals, etc., apart from pushing up costs of conducting business.

While cyber attackers gain increasing reach and power, legitimate business are set to suffer significantly. The ability to sell security products and compete globally might be impacted if the rules are adopted in current form and shape. Hence NASSCOM and DSCI request Bureau of Industry and Security to withdraw this proposal.

PUBLIC SUBMISSION

As of: 7/29/15 6:41 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-19gt
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0264

center for Technology democracy Andy Sayler 7-29

Submitter Information

General Comment

See attached

Attachments

center for Technology democracy Andy Sayler 7-29



July 20, 2015 -

Kevin Wolf
Assistant Secretary of Commerce for Export Administration
U.S. Department of Commerce

Hillary Hess
Director, Regulatory Policy Division
U.S. Department of Commerce

Catherine Wheeler
Director, Information Technology Controls Division
U.S. Department of Commerce

**Re: Comments on Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)**

Dear Assistant Secretary Wolf, Director Hess, and Director Wheeler:

On behalf of BSA | The Software Alliance (“BSA”),¹ we write to express the significant concerns of BSA members regarding the proposed rule, with request for comments, issued by the Commerce Department, Bureau of Industry and Security (“BIS”) in the *Federal Register* on May 20, 2015 (the “Proposed Rule”).

The Proposed Rule implicates complex technical and policy issues. BSA urges BIS to pause its current push to issue a final rule, and instead, take the additional time needed to fundamentally consider the proper scope and approach to these controls. Among other steps, BIS should convene technical workshops for input and insight from industry and the security community. After such fact-gathering, BIS should issue a new proposed rule that focuses on a narrower set of items and activities and avoids imposing undue compliance burdens on legitimate cybersecurity efforts. Once those consultations are completed, BIS should issue a second Notice of Proposed Rulemaking so that the cybersecurity community has the opportunity to review and provide comments on the revised rule.

¹ BSA’s members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Datastax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

If implemented as currently drafted, the Proposed Rule would seriously impair the ability of BSA members to identify and fix security vulnerabilities, while requiring thousands of export licenses. The net effect may well be to diminish security for individuals and enterprises because the sheer volume of activities covered under the Proposed Rule would impose unreasonable burdens on the processing capabilities of BSA member companies as well as BIS. As currently drafted, any intended benefits of the Proposed Rule would be overwhelmed by the untenable burdens that it would place on industry and BIS.

Most importantly, we believe the Proposed Rule would hamper the efforts of cybersecurity professionals to protect our nation's critical networks and infrastructure against malicious intrusion by imposing time delays and restricting the use of the best available tools to maintain security, while doing little to impede malicious hackers from obtaining and using tools for cyber intrusions. The Proposed Rule will likely undermine cybersecurity innovation as security researchers and companies alike will be required to seek approval for a broad range of work in a profession that demands its participants move in "Internet time." The Proposed Rule fails to appreciate the global nature of the security community and the important need for international collaboration, within a company and in the security research community. An inflexible regime that is based on nationality means that systems that need protection in real-time are not afforded the best protection available because of the need for licensing and approval.

I. The Overbroad Scope of the Proposed Rule Would Negatively Affect Cybersecurity

BSA understands that the original intent for these controls, when proposed for the Wassenaar Arrangement, was to restrict the export of sophisticated surveillance systems — such as those developed and sold by FinFisher and Hacking Team — to authoritarian governments, which reportedly have used these systems to spy on or otherwise repress political dissidents and other citizens.² BSA agrees that such systems, which permit the targeting and monitoring of an individual's phone calls, emails, and other communications, are appropriate items for tight export controls, implemented by the United States, the European Union, and other Wassenaar members.

By contrast, the scope of the Wassenaar controls as proposed for implementation in the Export Administration Regulations ("EAR") by BIS, would apply to a far broader range of items and activities. For example:

- *Technology Controls.* Export Control Classification Number ("ECCN") 4E001.c would control "technology" "required" for the "development" of "intrusion software." Because this ECCN entry lacks specific performance levels, much of the technology related to the development of intrusion software likely would qualify as "peculiarly responsible for

² See, e.g., Bill Marczak, Written Evidence to the UK Parliament, *Export of British-Made Spyware Targeting Bahraini Activists* (Nov. 19, 2012), available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmfaff/88/88vw43.htm>; Response of the UK Secretary of State for Business Innovation and Skills, *Export Controls for Surveillance Equipment - Proposed JR* (Aug. 8, 2012), available at https://web.archive.org/web/20140816043658/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_08_08_response_from_tsol.pdf.

achieving or exceeding the controlled . . . characteristics or functions” of “intrusion software,” and therefore would be considered “required” for its development. As a result this ECCN would describe an exceedingly large range of technologies, with virtually all exports and re-exports of such technology requiring an export license.

- *Software Controls.* Similarly, the proposed software controls in ECCN 4D004 attempt to limit their scope by only applying to software “specially designed” or modified for the generation, operation or delivery of, or communication with intrusion software, rather than intrusion software itself. However, BSA members report that all intrusion software that is developed for defensive/security purposes needs to be generated, delivered, and communicated with in the process of testing (and fixing) network and software security vulnerabilities. As such, BSA members report that they frequently develop and export software that would be controlled under ECCN 4D004 (as well as ECCN 4D001), both manually and through auto-code generation.

BSA appreciates the efforts that BIS has made to clarify the intended scope of the Proposed Rule, including the scope of these ECCNs, in a series of responses to Frequently Asked Questions (“FAQs”) on the BIS website. However, these FAQs are not reflected directly in the language of the Proposed Rule, and do not have the force of law. More importantly, even taking these FAQs into account, BSA members report that technology and software covered by these ECCNs are frequently generated by BSA members in the course of efforts to identify and fix network, software, and other security vulnerabilities, including critical cybersecurity work to protect our nation’s IT infrastructure. Because of the global nature of defensive security activities, and the wide involvement of security professionals of many nationalities, these activities require exports and re-exports to intra-company and third-party security teams in European and other countries, as well as “deemed exports” to non-U.S. nationals (lawfully working in the U.S.) and “deemed re-exports” to dual and third-country nationals lawfully working in non-U.S. countries. Moreover, these deemed exports and re-exports must occur globally and within minutes, given that vulnerabilities or threats may require tooling, software, and expertise to move as quickly as the threat.

II. The Proposed Rule Would Result in Thousands of Export License Applications

The burden of complying with the Proposed Rule would be substantial. As drafted, the rule would require licenses for virtually all exports, re-exports, and deemed exports of an overly-broad set of controlled items. Some BSA members have projected that, if the Proposed Rule is adopted, their individual companies would likely be required to obtain thousands of export and/or deemed export licenses. The number of licenses required across all BSA member companies would be much larger, and the projected number of activities and tools subject to licensing controls in the software and IT industries would be staggering. It would bring development and testing to a standstill, as the backlog of licensing requests would quickly balloon to an unmanageable level. This volume is unmanageable for even the largest companies’ Trade Compliance departments, and even more importantly, BIS does not have nearly enough capacity to process these license applications.

It is also worth noting that many in the security researcher community lack the resources necessary to comply with the Proposed Rule. Much of the cutting edge work in the

cybersecurity field is performed by sole practitioners, small businesses, and academics. These entities are unaccustomed to the complexities of the export licensing process, and the delays and costs of complying with the Proposed Rule will significantly undermine their ability to participate in the cybersecurity ecosystem. Because many enterprises, including BSA members and governments, rely on their contributions, the impact on the security community will be widespread.

The Proposed Rule will make it exceedingly difficult for industry to identify and segregate controlled from non-controlled technology in the context of ongoing cybersecurity efforts; as such, industry will be forced to be over-inclusive when identifying controlled technology. Furthermore, an exporter would only need to anticipate sharing a single piece of controlled technical data with a foreign national for the export or deemed export licensing requirement to apply. The broad scope of the controls, and the ambiguities that remain even after multiple issuances of FAQs and answers, thus contributes to the massive projected licensing volume that would be created by the Proposed Rule.

The licensing burden results not only from the overbroad scope of the Proposed Rule, but also because the Proposed Rule does not offer any eligibility for license exceptions. For example, the Proposed Rule does not authorize mass-market software exports under License Exception TSU. The Proposed Rule likewise would not authorize exports of software or technology with a written assurance and appropriate compliance measures under License Exception TSR. License Exception ENC also would not be available for cybersecurity items that perform encryption.

It is important that BIS create new license exception(s) to enable legitimate and critical cybersecurity activities, such as intra-company transfers or transfers with third-party partners for security research activities. Such license exceptions are entirely consistent with U.S. participation in the Wassenaar Arrangement. The Wassenaar Arrangement is a forum for member states to agree on *what* is controlled. As explicitly stated in the Wassenaar *Initial Elements*, the decision on *how* to control the export of a controlled item is left to “national discretion.”³ Indeed, the European Union has already implemented the Wassenaar controls,⁴ including the availability of general licenses for certain exports (and subject to compliance with certain additional requirements).

BIS should also reconsider the “policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities.” Because most, if not all, end point security products contain some degree of rootkit functionality, a presumption of license denial will impede the ability of cybersecurity professionals to use and exchange a broad range of products and tools that are critical to protecting networks from intrusion. Restricting the exchange of items containing zero-day vulnerabilities and associated exploit capabilities will have a similar effect. Cybersecurity professionals engage in penetration testing for purposes of identifying and remediating network vulnerabilities and exploits. The tools used in penetration testing exercises

³ See Wassenaar Arrangement, *Initial Elements*, Section II.3, available at <http://www.wassenaar.org/guidelines/docs/5%20-%20Initial%20Elements.pdf>.

⁴ See Regulation (EU) No 1382/2014 (effective as of Dec. 31, 2014).

make use of zero-day vulnerabilities and then help to develop exploits to assess those vulnerabilities. The research and software engineering necessary to remediate those exploits is conducted in hours and is international in scope. To effectively close those network vulnerabilities, companies must be able to share freely and in real time. The inability to freely share the vulnerabilities and exploits that the penetration testing tools find, due to their zero-day exploit capabilities, will severely impact the ability to create safe products and ensure a secure network and IT environment.

III. BIS Should Fundamentally Rethink the Approach to these Controls and Issue a Second Proposed Rule

BSA recognizes that the goal of the Proposed Rule is to protect human rights by preventing rogue actors from undermining cybersecurity. However, by imposing enormously burdensome requirements on fundamental network security tools and practices, the Proposed Rule is likely to have the opposite effect. Securing systems and individuals against exploits, vulnerabilities, intrusions, and threats requires real-time testing and remediation actions. Such efforts must occur immediately upon the detection of a vulnerability or intrusion. As drafted, the Proposed Rule would impose burdens that will inevitably delay testing and remediation, and thus diminish security in a very real way. Both product development and security response will be stymied, as approval will be needed at each step of the process. Such an outcome would be at odds with the Obama Administration's broader cybersecurity policy, which recognizes that "private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible."⁵

Given the complexity of the technical and policy issues raised by the Proposed Rule, BSA urges BIS, along with its inter-agency partners, to pause any current rush to issue a final rule. BIS should take the time to fundamentally rethink the approach taken to these controls -- i.e., whether to revisit the scope of the controls at Wassenaar; to issue Technical Notes, definitions, lists of excluded items within ECCN entries; or other options for appropriately drawing the scope of these controls. This also could include BIS hosting technical seminars or workshops with industry and the security community.

In the process of this engagement, BIS may identify novel approaches -- which satisfy the needs of both the U.S. Government, industry, and other organizations -- to regulation in this complex area. For example, as BIS did with encryption exports, and as implemented by the EU, there may be a registration-based approach for cybersecurity items that avoids the need for individual licensing. Alternatively, there may be end-user or end-use-based controls that more effectively control the sensitive activities of interest to the U.S. Government, without over-controlling non-sensitive, security *enhancing* activities. Such an approach could differentiate between "white hat" developers who are seeking to improve security across the ecosystem and "black hat" hackers who are focused on substantially harming an information system or data on

⁵ Executive Order 13691.

an information system. A use-based focus could help to ensure that the export control licensing requirements are not undermining the time sensitive efforts of cybersecurity professionals. However it is constructed, the final rule should be minimally invasive and maximize the ability of the security community to innovate and respond to threats and global challenges.

Once this work is complete, BIS would be in a position to issue a second proposed rule, as has been done with other complex Export Control Reform rulemakings. This second proposed rule should clearly describe the (much narrower) scope of controlled items, without reliance on FAQs on the BIS website (which do not have the force of law) and provide an opportunity for further commentary as needed.

BSA and its members welcome the opportunity to engage further with BIS, and all other interested departments and agencies, on these complex technical and policy issues.

**Comments to the U.S. Department of Commerce on
Implementation of 2013 Wassenaar Arrangement Plenary Agreements**

(RIN 0694-AG49)

July 20th, 2015

Submitted by

Access,
Center for Democracy & Technology,
Collin Anderson,
Electronic Frontier Foundation,
Human Rights Watch &
New America's Open Technology Institute¹

*Access, the Center for Democracy & Technology, Collin Anderson, the Electronic Frontier Foundation, Human Rights Watch, and New America's Open Technology Institute respectfully submit these comments to the U.S. Department of Commerce in response to the Bureau of Industry and Security's Request for Comments on Wassenaar Arrangement 2013 Plenary Agreements Implementation.*²

Access is an international, non-profit organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

The Center for Democracy & Technology (CDT) is a nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways.

Collin Anderson is a Washington, D.C.-based computer scientist focused on Internet controls and restrictions on communications, including network

¹ Contact Laura Moy, Senior Policy Counsel, Open Technology Institute, moy@newamerica.org.

² Bureau of Industry and Security, "Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items," *Federal Register* Vol. 80 No. 97, May 20, 2015, <https://federalregister.gov/a/2015-11642> (80 FR 28853).

ownership, disruption of access and regulatory regimes, with an emphasis on countries that limit the free flow of information.

The Electronic Frontier Foundation (EFF) is a nonprofit, member-supported civil liberties organization working to protect privacy and free expression in technology, law, policy, and standards in the information society. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With over 21,000 dues-paying members and over 284,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

Human Rights Watch (HRW) is an independent global organization that monitors human rights in more than 90 countries around the world. HRW defends the rights of people worldwide by scrupulously investigating abuses, exposing the facts widely, and pressuring those with power to respect rights and secure justice.

New America is a nonprofit, nonpartisan public policy institute based in Washington, D.C. that invests in new thinkers and new ideas to address the next generation of challenges facing the United States and the global community. The Open Technology Institute is a program within New America that promotes affordable, universal access to open and unrestricted communications networks through technology development, applied learning, and policy reform.

I. Introduction

We sincerely thank the Bureau of Industry and Security (BIS) of the Department of Commerce for taking the time to solicit public comments on the proper implementation of the 2013 Wassenaar controls related to Intrusion and IP Network Surveillance Items. We hope the opportunity for public comment helps BIS to better understand how the proposal will impact the information and communications technology market and related technical communities.

The organizations that we represent are familiar not only with the technical elements of the proposed rule, but also with the human rights concerns that led the French and UK governments to propose the original controls in 2013. The goal of our comments is both to provide specific information about aspects of the rule that are either ambiguous or otherwise concerning, and to offer concrete recommendations to address these problems. We believe it is possible for Commerce to craft a final rule that is narrowly tailored to address the human rights concerns raised by the spread of the single-use surveillance technologies without

adversely affecting a variety of additional technologies, including important security research and testing tools.

These comments are structured as follows:

- **Part II** describes the policy challenge that the original Wassenaar controls related to Intrusion Software and IP Network Surveillance Systems sought to control and the wide range of evidence that has emerged in recent years about the human rights abuses that are facilitated by the export of these technologies to repressive regimes;
- **Part III** describes the original scope and intent of the surveillance-related controls adopted by the members of the Wassenaar Arrangement at the 2013 Plenary meeting;
- **Part IV** offers a number of recommendations for how BIS can tailor its approach to address concerns about overbreadth without sacrificing the important policy goal of addressing the human rights abuses facilitated by the export of these technologies, including:
 - Apply the Technology and Software – Unrestricted (TSU) license exception to cybersecurity software.
 - Issue broad license authorizations for transfers of penetration testing software and hardware that does not qualify for license exceptions to non-governmental use and users.
 - After adopting license exception TSU and broad license authorizations for non-governmental use and users, tailor the licensing process for remaining items specifically to human rights concerns regarding cybersecurity items.
 - Provide guidance on the “generation” component of ECCN 4D004 to decontrol certain classes of development tools.
 - Narrow the control on technology for the “development” of Intrusion Software so that it only applies to transfers to government end users or for military or law enforcement purposes.
 - Provide clear “Know Your Customer” guidance.
 - Issue clear guidance on key terminology introduced into the text of the rule.
 - Establish a transparent and iterative process to assess the success of the rule after it has been applied and adjust it as necessary to address possible over- or under-breadth.

II. The Policy Challenge: Human Rights Abuses Facilitated by the Export of Surveillance Technology to Repressive Regimes

The uncontrolled export of surveillance technologies to countries with dubious human rights records poses a growing, significant threat to fundamental rights and the free flow of information online.³ These tools – commonly marketed directly to governments and designed to build surveillance and privacy-invasion capabilities into a country’s communications infrastructure – not only undermine the work of human rights groups and journalists to hold governments democratically accountable, but also endanger the daily lives of individual citizens. After the revolutions that swept the Arab world in 2011, archives obtained from those fallen regimes showed that a number of Western companies had been supplying censorship and surveillance technology to these and other repressive governments despite their poor human rights records.⁴ These revelations have subsequently been supported by extensive research from a variety of academic institutions and human rights organizations, including the University of Toronto’s Citizen Lab, Reporters Without Borders, Access, Human Rights Watch, and Privacy International.⁵ Recently-leaked documents describing the operations of Hacking

³ These fundamental rights include, *inter alia*, the right to privacy and the right to freedom of expression, which are affirmed and protected by the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR), which the U.S. has ratified. Recent interpretations of these rights are found in: Human Rights Committee, “General Comment 34,” 2011, <http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>; Navi Pillay, UN High Commissioner for Human Rights, “The Right to Privacy in the Digital Age,” 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; reports by Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in 2011, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf, and 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf; and his successor Special Rapporteur David Kaye, in 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.

⁴ See, e.g., Karen McVeigh, “British firm offered spying software to Egyptian regime – documents,” *The Guardian*, April 28, 2011, <http://www.theguardian.com/technology/2011/apr/28/egypt-spying-software-gamma-finisher>; Paul Sonne & Margaret Coker, “Firms Aided Libyan Spies,” *The Wall Street Journal*, August 30, 2011, <http://www.wsj.com/news/articles/SB10001424053111904199404576538721260166388>; “Syria Crackdown Gets Italy Firm’s Aid With U.S.-Europe Spy Gear,” *Bloomberg Business*, November 3, 2011, <http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear>; Vernon Silver, “Hewlett Packard Computers Underpin Syria Surveillance Project,” *Bloomberg Business*, November 18, 2011, <http://www.bloomberg.com/news/articles/2011-11-18/hewlett-packard-computers-underpin-syria-electronic-surveillance-project>; Trevor Timm & Jillian C. York, “Surveillance Inc: How Western Tech Firms Are Helping Arab Dictators,” *The Atlantic*, March 6, 2012, <http://www.theatlantic.com/international/archive/2012/03/surveillance-inc-how-western-tech-firms-are-helping-arab-dictators/254008/>.

⁵ See, e.g., Morgan Marquis-Boire, et al., “Planet Blue Coat: Mapping Global Censorship and Surveillance Tools,” *The Citizen Lab*, January 15, 2013, <https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/>; Morgan Marquis-Boire, et al., “Some Devices Wander By Mistake: Planet Blue Coat Redux,” *The Citizen Lab*, July 9, 2013, <https://citizenlab.org/2013/07/planet-blue-coat-redux/>; “The Enemies of the Internet: Corporate Enemies,” *Reporters Without Borders*, March 2013, <https://surveillance.rsrf.org/en/category/corporate-enemies/>; “Commonwealth of Surveillance States,” *Access*, June 2013, https://s3.amazonaws.com/access.3cdn.net/279b95d57718f05046_8sm6ivg69.pdf; “Ethiopia: Telecom Surveillance Chills Rights: Foreign Technology Used To Spy on Opposition Inside the Country, Abroad,” *Human Rights Watch*, March 25, 2014, <https://www.hrw.org/news/2014/03/25/ethiopia->

Team, an Italian vendor of Intrusion Software, provide further evidence of the proliferation of Western surveillance technologies to repressive countries, with notable clients such as Azerbaijan, Bahrain, Ethiopia, Kazakhstan, Nigeria, Oman, Saudi Arabia, and Uzbekistan, as well as sanctioned states like Sudan and Russia.⁶

As this evidence has emerged in the past few years, human rights advocates and policymakers have explored various ways to hold accountable American and European companies that develop and sell these products when they facilitate human rights abuses. Some businesses in the United States, United Kingdom, and France have faced legal challenges for violating human rights under existing domestic laws.⁷ While these efforts have generated significant media attention, their efficacy as a legal strategy to actually provide redress against the companies selling these technologies – particularly in the U.S. – has been less clear.

Consequently, another proposal that has gained some support is to use export controls to curb the unfettered proliferation of such technologies to countries with dubious human rights records and give the government a clear path to penalize the companies that violate these regulations.⁸ Making a narrow and specific group of technologies subject to a licensing regime for review prior to export – based on their technical characteristics as well as their destination and likely end-use – is one potential avenue to address important human rights concerns created by the proliferation of monitoring and censorship technology.⁹

[telecom-surveillance-chills-rights](https://www.privacyinternational.org/?q=node/293); “Private Interests: Monitoring Central Asia,” *Privacy International*, November 2014, <https://www.privacyinternational.org/?q=node/293>.

⁶ See, e.g., Sarah Myers West, “Hacking Team Leaks Reveal Spyware Industry’s Growth, Negligence of Human Rights,” *Electronic Frontier Foundation*, July 8, 2015, <https://www.eff.org/deeplinks/2015/07/hacking-team-leaks-reveal-spyware-industrys-growth>; Joshua Kopstein, “Here Are All the Sketchy Government Agencies Buying Hacking Team’s Spy Tech,” *Motherboard*, July 6, 2015, <http://motherboard.vice.com/read/here-are-all-the-sketchy-government-agencies-buying-hacking-teams-spy-tech>.

⁷ In 2012, the French government opened up a judicial inquiry against Amesys, a division of the French company Bull, to look into its operations in Libya after two human rights groups filed formal complaints about the alleged sale of surveillance systems to the Qaddafi regime. Ryan Gallagher, “French Company That Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations,” *Slate*, June 19, 2012, http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi.html; for more details on the formal complaint, see “Opening of a judicial inquiry targeting Amesys for complicity in acts of torture in Libya,” FIDH, May 24, 2012, <https://www.fidh.org/International-Federation-for-Human-Rights/north-africa-middle-east/libya/Opening-of-a-judicial-inquiry>. In the United States, Cisco has been sued for selling equipment to the Chinese government that was used as part of its censorship and surveillance regime. Rainey Reitman, “Cisco and Abuses of Human Rights in China: Part 1,” *Electronic Frontier Foundation*, August 22, 2011, <https://www.eff.org/deeplinks/2011/08/cisco-and-abuses-human-rights-china-part-1>.

⁸ Danielle Kehl & Tim Maurer, “Against Hypocrisy: Updating Export Controls for the Digital Age,” *CyberDialogue*, March 9, 2013, <http://www.cyberdialogue.ca/2013/03/against-hypocrisy-updating-export-controls-for-the-digital-age-by-danielle-kehl-and-tim-maurer/>.

⁹ For an in-depth discussion, see Tim Maurer, Edin Omanovich, and Ben Wagner, “Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age,” *New America’s Open Technology Institute, Privacy International & Digitale Gesellschaft*, March 2014, <http://www.newamerica.org/oti/uncontrolled-global-surveillance-updating-export-controls-to-the-digital-age/>.

The idea of using trade restrictions to address human rights concerns related to communications technologies is not without precedent in the United States. Indeed, the U.S. exercises broad sanctions against particular countries for human rights abuses. Since 2010, the U.S. government has maintained additional prohibitions on exporting “sensitive technology” to Iran, which includes hardware, software, and telecommunications equipment that can be used “to restrict the free flow of unbiased information” or “disrupt, monitor or otherwise restrict speech.”¹⁰ The sensitive technologies language represents an acknowledgement by the U.S. government that surveillance and censorship technologies are often abused by repressive regimes, and that penalties for companies caught exporting such tools should be severe. In 2012, the United States also began restricting the export of IMSI catchers – devices that enable “man in the middle attacks” and intercept mobile phone traffic by impersonating cell phone towers – after similar language was adopted by the Wassenaar Plenary.¹¹

This approach is not without risks, however. There has long been apprehension about export controls among those in the technical community who remember the “Crypto Wars” of the 1990s: an infamous battle over the broad and messy restrictions placed on cryptography exports.¹² Although the United States has relaxed most limits on the export of encryption since 1999, further liberalization of encryption controls is still required and similar concerns about complexity and the risk of overreach with export controls should not be overlooked. The language used to describe the scope of the systems being controlled needs to be flexible enough to catch the targeted products, while at the same time specific enough to ensure that other tools and services are not inadvertently covered.¹³ Achieving this delicate balance is critically important for security researchers and professionals, especially since it can be challenging to differentiate between defensive products used to protect systems and those that are used to compromise them.

Export controls are not a panacea and their application will neither eliminate the trade in censorship and surveillance technologies, nor mitigate threats posed by

¹⁰ Christopher M. Matthews, “State Department Clarifies ‘Sensitive Technologies’ Sanctions,” *The Wall Street Journal*, November 13, 2012, <http://blogs.wsj.com/corruption-currents/2012/11/13/state-department-clarifies-sensitive-technology-sanctions/>.

¹¹ Jamie Doward & Rebecca Lewis, “UK ‘exporting surveillance technology to repressive nations,” *The Guardian*, April 7, 2012, <http://www.theguardian.com/world/2012/apr/07/surveillance-technology-repressive-regimes>; *Federal Register* Vol. 77 No. 127, July 2, 2012, http://www.bis.doc.gov/index.php/forms-documents/doc_view/577-77-fr-39353 (describing changes to Category 5, Part 1 – Telecommunications).

¹² For an in-depth discussion of the history of U.S. export controls on cryptography, see Section III, “The Battle Over Encryption Export Controls,” in Danielle Kehl, Andi Wilson & Kevin Bankston, “Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s,” *New America’s Open Technology Institute*, June 2015, <http://www.newamerica.org/oti/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/>.

¹³ Edin Omanovich, “Export Controls and the Implications for Security Research Tools,” *Privacy International*, December 8, 2013, <https://privacyinternational.org/?q=node/354>.

producers of such systems located in countries not subject to the Wassenaar Arrangement. Surveillance technologies produced within countries that are members of the Wassenaar Arrangement, however, are often more sophisticated than the other systems available in the international marketplace and therefore warrant additional scrutiny. Properly-implemented export controls can be a valuable tool to help curb the unregulated spread of these systems and promote broader norms, which is important not only given the United States' role in the international sale of Intrusion Software and IP Network surveillance technologies, but also its leadership in promoting Internet Freedom and responsible business and human rights practices. Even when they are not invoked to restrict a transfer of surveillance technology, export controls also act as an essential accountability and transparency mechanism. Greater transparency into this industry can assist the U.S. government in monitoring the human rights impact of U.S. businesses and improving policies to address abuses and enhance remedies where companies cause or contribute to human rights harms.

III. Surveillance-Related Controls Adopted by the Members of the Wassenaar Arrangement at the 2013 Plenary Meeting

At the conclusion of the 2013 Wassenaar Plenary meeting, its members announced that they were adopting new controls relating to “Intrusion Software” and “IP network surveillance systems.”¹⁴ “Intrusion Software” is designed to surreptitiously intercept activities and communications on electronic devices, such as passwords, screenshots, microphone recordings, camera snapshots, and Skype chats, and to remotely execute commands. “IP network surveillance systems” constitute mass surveillance platforms – systems to monitor general network traffic for large populations of Internet users in order to identify and collect information about those users. It is clear from the language used in the Wassenaar Plenary Agreements, the motivations of the member states that brought the original proposals, and BIS’s justification of the imposition of the National Security control that the intent of the new controls is to restrict the sale of systems that can be used to commit human rights abuses.

When these new controls were announced, a number of human rights organizations supported the decision to control a specific set of single-use surveillance technologies, recognizing the incorporation of human rights considerations into the discussions at a traditionally security-focused forum like

¹⁴ Edin Omanovich, “International Agreement Reached Controlling Export of Mass and Intrusive Surveillance Technology,” *Privacy International*, December 8, 2013, <https://privacyinternational.org/?q=node/398>.

the Wassenaar Arrangement as a step forward.¹⁵ A number of academics and civil society organizations also submitted proposed guidance to the agencies responsible for implementing export controls nationally (both in the United States and the European Union), advising them on what to consider when implementing the controls.¹⁶

At the same time, however, many human rights organizations recognized that there were risks that the proposed controls could be interpreted in an overbroad manner. In addition to urging the relevant agencies to implement the new controls outside of existing encryption controls, these groups placed heavy emphasis on concerns about how the controls associated with Intrusion Software could impact security research if implemented in an overbroad manner. Moreover, these comments stressed the importance of the General Software Note and General Technology Note in preventing a chilling effect on essential security practices and the development of information security tools by exempting open source systems, research, and mass-market security software from these regulations.¹⁷

For example, recommendations published by Access, Collin Anderson, Internews, Reporters Without Borders, and New America's Open Technology Institute in May 2014 advised U.S. government agencies involved in implementing the controls that:

- “Protecting research and general purpose computing is critical to promoting Internet security, and new controls should be implemented in a manner that aligns with existing technology and software exemptions. We recommend that Wassenaar’s ‘General Technology Note’ and ‘General Software note under the Technology and Software – Unrestricted exemption’ are replicated explicitly in American regulations for Intrusion Software.”¹⁸

¹⁵ See, e.g., “International Body Moving to Restrict Export of Surveillance Systems Used to Commit Human Rights Abuses,” *New America’s Open Technology Institute*, December 9, 2013, <https://www.newamerica.org/oti/international-body-moving-to-restrict-export-of-surveillance-systems-used-to-commit-human-rights-abuses/>.

¹⁶ “Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding ‘Intrusion Software’ and ‘IP Network Communications Surveillance Systems,’” Submitted by Access Now, Collin Anderson, Internews, Reporters Without Borders, and New America’s Open Technology Institute, May 5, 2014, <http://www.newamerica.org/oti/human-rights-and-technology-organizations-submit-joint-recommendations-to-the-us-government-on-the-implementation-of-the-2013-wassenaar-amendments-on-surveillance-technology/> (“Joint Civil Society Recommendations for U.S. Implementation”).

¹⁷ See Collin Anderson, “Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies,” Access, March 2015, <https://s3.amazonaws.com/access.3cdn.net/f3e3f15691a3cc156ae1m6b9vib.pdf>. In particular, “There is indication that special care was taken to limit potential overreach in the drafting of the Intrusion Software control. For example, the definition attempts to mitigate over-breadness through defining a set of exemptions, as well as not directly controlling Intrusion Software itself. Additionally, while the majority of the Wassenaar Arrangement’s Controls for Technology cover the ‘development, production, or use’ of controlled systems, the Intrusion Software’s Technology controls only covers ‘development’ [4. E. 1. c.]”

¹⁸ Joint Civil Society Recommendations for U.S. Implementation, 3.

- “In contrast to the technical specificity of IP network surveillance, the controls outlined for Intrusion Software could potentially be interpreted broadly... to include more than commercial surveillance technologies. Intrusion controls should not threaten the public’s ability to control personal devices or prevent researchers from engaging in security auditing, even where it may include the discovery of vulnerabilities . . . [O]verbroad language could intentionally or inadvertently be used to stifle jailbreaking, security research, and additional activities that would otherwise promote privacy or general purpose computing.”¹⁹

Anticipating the risks of overbreadth, the 2013 Wassenaar Plenary includes several provisions aimed at ensuring that the proposed controls are appropriately tailored in their application, exempting commercial and research technologies. This reflects Wassenaar’s goal of controlling the export of technology to nation-state level actors while avoiding interfering with mass-market software and systems. In particular, the agreement includes both the General Technology Note and the General Software Note. These decontrol notes are available to the 2013 Wassenaar “Intrusion Software” categories (4.A.5, 4.D.4, and 4.E.1.c) as well as to the 2013 Wassenaar “Network Surveillance” category (5.A.1.j). Indeed, such exceptions are critical to ensuring that the new categories are not asserted in an overboard manner.²⁰

IV. Recommendations for Implementation of the Wassenaar Arrangement 2013 Controls on Intrusion Software

As the Bureau of Industry and Security considers ways to tailor its proposed implementation of the Wassenaar Arrangement 2013 controls to address concerns about overbreadth articulated by security researchers, we offer a number of recommendations to assist with that goal, detailed in this section.

The overarching objectives of our recommendations are to narrow application of the rule only to those circumstances that implicate the human rights and foreign intelligence concerns that provoked the original proposals, to ensure that the licensing policies applied to otherwise inflexible control language strongly protect against the provision of technologies that will contribute to the infringement of fundamental rights, and to reduce the likelihood of adverse effects on security research and practices. The proposals brought by the French and UK governments to the Wassenaar Plenary in 2013 sought to control platforms and technologies

¹⁹ *Id.*, 10.

²⁰ Anderson, “Considerations on Wassenaar Arrangement Control List Additions for Surveillance Technologies.”

designed to perform the remote compromise of communications devices or mass interception of traffic for the purposes of surveillance.²¹ We urge BIS to maintain that focus.

We also believe that the final rule will require further clarification from BIS on the scope and language of the controls, bearing in mind that the current draft rule affects communities (e.g. security researchers and independent software developers) that have not traditionally interacted with the export control system and may need assistance navigating the complexities of the Export Administration Regulations. It is also important to note that many of these individuals and smaller commercial entities may not have the resources to adequately handle the licensing process.

A. “Cybersecurity Software” should be subject to license exception TSU

The 2013 Wassenaar language applies the General Software Note decontrol language to all of the newly proposed 2013 Cybersecurity Items.²² Traditionally, BIS has implemented the mass-market provisions of the General Software Note via the TSU (Technology and Software - Unrestricted) license exception.²³ However, the proposed implementation of the new categories explicitly excludes the Cybersecurity Items from license exception TSU via proposed sub-section 740.13(d)(2)(ii).²⁴ BIS asserts that this “cybersecurity software” TSU exclusion is necessary to stay “consistent with the existing encryption exclusion” because “software described in the new control list entries may incorporate encryption functionality.”²⁵ This interpretation, however, risks an overbroad application of the new controlled categories, triggering many of the concerns raised by the security research and practitioner community regarding the proposed rule. Such an

²¹ In prior publications, researchers identified a number of vendors of such products, including for Intrusion Software: FinFisher (formerly Gamma Group), Hacking Team, DigiTask, AGLAYA, RCS Lab, Gr Sistemi (Dark Eagle), Clear-Trail Technologies (QuickTrail), Stratign (Spy Phone), SS8 (Interceptor), iPS (ITACA); for IP Network Surveillance: ETI Group’s EVIDENT Investigator, SS8 Communications Insight (Intellego), Area SpA MCR Studio, Amesys’s EAGLE GLINT (Nexa Technologies SAS), AMECS’s Analys, Narus nSystem, Vastech ZEBRA, Group 2000’s Lawful Monitoring Centre, Glimmerglass CyberSweep Sapience, ATIS Klarios Monitoring Centre, Siemens Intelligence Platform, Verint Systems, AQSACOM Aquamen, Nice Systems. see *Access, supra*.

²² WA-LIST (13) 1 04-12-2013, 3.

²³ 15 CFR 740.13; Separately, the “public domain”, “fundamental research”, and related components of the General Software and General Technology Notes are codified via 15 CFR 734.3.b.3.

²⁴ 80 FR 28853. “§ 740.13—license exception TSU”; While the public domain and fundamental research exemptions remain available to “cybersecurity software” via 734.3.b.3, mass-market software that does not qualify for such exemptions (e.g. because it is not freely available) that would otherwise be eligible for the General Software Note exemption will not be able to take advantage of the TSU exemption under the rules as currently proposed.

²⁵ 80 FR 28853. “§ 740.13—license exception TSU”; BIS Intrusion and Surveillance Items FAQ #23, available at <https://www.bis.doc.gov/index.php/policy-guidance/faqs>.

interpretation also fails to reflect existing issues with the restriction on license exception TSU for encryption software.

Furthermore, the proposed TSU exclusion does not align with the intended Wassenaar interpretation or other countries' implementations of the rules. Multi-national control regimes such as Wassenaar are most effective when all involved countries interpret and implement the rules consistently. Since many of the systems the new rules aim to control are manufactured by non-U.S. companies, deviating from the General Software Note by adding additional restrictions to only the U.S. implementation of the rules amounts to a unilateral control, which will do little more than unduly burden U.S. companies and researchers without serving any additional human rights interests.²⁶

BIS should therefore apply license exception TSU to the proposed "cybersecurity software" categories.²⁷ A license exception for mass-market cybersecurity software will help ensure that the new control categories do not adversely affect the distribution of penetration testing tools, network security tools, or other categories of items that may be inadvertently caught by these controls – and will address many of the deemed export and inter-company/university transfer issues that threaten to create an onerous burden on international companies and educational institutions. This conclusion is based on the following considerations:

1. *Mass-market cybersecurity software does not present as substantial a threat to human rights as systems designed for and marketed to state-level actors.*

The Wassenaar Arrangement is designed to control the sale of software to nation-state level actors. To the extent that software is generally available on the mass market, via either the publication of source-code or the provisions outlined under the TSU, it should not be controlled by Wassenaar.

Decontrolling mass-market software will not run contrary to the objectives of the proposed rule. The controls, as originally conceived, were intended to exercise oversight over the proliferation of technologies that are primarily marketed toward law enforcement, judicial bodies, military entities, and state-level intelligence agencies. These Intrusion Software and Network Surveillance items have a more limited customer market, and are reliant on continued vendor support and opacity for continued effectiveness against security countermeasures. A review of the client lists, sales documents and statements associated with companies that are

²⁶ See Maily Fidler, "Proposed U.S. Export Controls: Implications for Zero-Day Vulnerabilities and Exploits," April 2014, <http://www.lawfareblog.com/proposed-us-export-controls-implications-zero-day-vulnerabilities-and-exploits>.

²⁷ WA-LIST (13) 1 04-12-2013, 3.

believed – or have themselves acknowledged – to be controlled under the proposed rules describes an industry with a limited customer base due to the high cost of such systems and added transactional discretion not characteristic of mass-market items.²⁸

2. *Overlap between encryption and cybersecurity software does not negate the need to extend the TSU exception to cybersecurity software.*

It has been suggested that there is no need to apply license exception TSU to cybersecurity software because many tools used by security researchers are already controlled under the existing Category 5, Part 2 encryption controls, and as such are excluded from the General Software Note and consequently the TSU exception as well. Although we recognize that there may be some overlap between the cryptographic controls and cybersecurity software, we nevertheless believe that the TSU exception must be extended to cybersecurity software. Such an extension is necessary to address concerns that the proposed rules will adversely affect the availability of penetration testing and network security tools commonly used by security researchers.²⁹ Software such as CANVAS, Metasploit, and CORE Impact provide not only direct security auditing for companies, but are also used by outside contractors to test network intrusion detection systems, audit networks for vulnerabilities, and test protective measures. To the extent that these tools support cryptography, such functionality is largely ancillary to the primary purpose of the tools – they are not primarily intended for encrypted communications or cryptanalytics.

Moreover, there are identifiable cases of software and technology that appear to fall into a grey area with the proposed controls but do not include encryption. These include development suites that are used for the generation of exploits and malware.³⁰ As such, it is not clear that such tools would even be subject to the existing Category 5, Part 2 cryptographic controls in force today. Consequently, it does not make sense to subject all such tools to the existing restrictions on license exception TSU applied to the Category 5, Part 2 items.

²⁸ See Anderson, “Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies,” 10-19, 23-29.

²⁹ See, e.g., Nate Cardozo and Eva Galperin, “What is the U.S. Doing About Wassenaar and Why Do We Need to Fight It?” *Electronic Frontier Foundation*, May 28, 2015, <https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation>; Kim Zetter, “Why An Arms Control Pact Has Security Experts Up in Arms,” *WIRED*, June 24, 2015, <http://www.wired.com/2015/06/arms-control-pact-security-experts-arms/>.

³⁰ See, e.g., technologies described in “Intro,” <https://lists.alchemistowl.org/pipermail/regs/2015-June/000173.html>.

3. *The application of license exceptions should take into account the evolving role of cryptography in modern technologies.*

Although the question about whether export controls should apply to encryption technology is outside of the scope of the current request for comments, we urge the Commerce Department to recognize that such controls are also problematic for a variety of reasons, and that the new rule should not be structured in such a way that perpetuates the challenges created by these restrictions.³¹ Given the issues with the existing General Software Note and related EAR carve-outs for encryption, it would be inappropriate to continue to apply these mechanisms to the newly proposed categories.

Encryption is quickly becoming a standard feature in all modern software and digital services and a norm among rights-respecting information and communications technology providers.³² From communication systems to data storage and beyond, almost all modern software solutions recognize the importance of employing cryptographic techniques in order to protect and verify the information users generate and provide. Thus, the number of systems that risk being swept up under the controls in the existing Section 5, Part 2 restrictions is rapidly growing. Even with the myriad of reforms passed during the previous 20 years, the complexity of the rules and license exceptions surrounding cryptography in the EAR remains inaccessible to the vast majority of individuals creating software and sharing or selling it online. Much of this existing complexity and the chilling effects it promotes could be resolved by simplifying the current patchwork of license exceptions and carve-outs surrounding Category 5, Part 2.³³

Although these challenges cannot be resolved entirely within the scope of this proceeding, BIS can at the very least ensure that the cybersecurity items are not subject to the same set of problematic restrictions. These policies should recognize

³¹ This recommendation is consistent with previous recommendations that the new controls should be implemented outside of existing controls on encryption technology. See, e.g. Joint Civil Society Recommendations for U.S. Implementation, Part II (“Controls for Surveillance Technology Should Be Implemented Independent of Existing Encryption Controls”), 7-9.

³² For example, the U.S. government recently mandated the use of encryption on all government websites and services (see <https://https.cio.gov/>). Furthermore, almost all major operating systems (e.g. Linux, Android, OSX, iOS, and Windows), storage technologies (e.g. the Ext4 filesystem (see <https://lwn.net/Articles/639427/>), Dropbox (see <https://www.dropbox.com/en/help/27>), etc), and communication systems (e.g. Google’s end-to-end (see <https://github.com/google/end-to-end>), TextSecure (see <https://whispersystems.org/>), etc) now offer various forms of cryptographic capabilities.

³³ In particular, the Wassenaar Arrangement should be amended to apply mass-market and publication exceptions of the General Software Note to all encryption related controls. Similarly, the EAR should be amended to apply the 15 CFR 734.3.b and 15 CFR 740.13.d (TSU) provisions to all Category 5, Part 2 items. Such modifications would help end the current patchwork rules and requirements and remove the burdensome the registration requirements for those writing encryption-related code (which may soon include essentially all computer code).

the evolving role of encryption in modern communications tools and systems, and offer a broader range of exemptions, including those offered under license exception TSU. In doing so, BIS will also lay the groundwork for better licensing policies on software with encryption functionality in the future.

4. *Broad license exceptions will protect cybersecurity research practices and minimize concerns about scope.*

Unfettered access to mass-market and publicly available cybersecurity tools is critical to ensuring that security researchers and practitioners can adequately test systems and harden them to defend against malicious intrusion. Security researchers and professionals must be able to freely share documentation of attacks, exploit code, and exploit frameworks for purposes of penetration testing, fixing bugs, advancing protective practices, and other activities.

The free flow of this information promotes security. For example, the recent leak of the source code for Hacking Team's Intrusion Software platform has led to numerous fixes for vulnerabilities that attackers were previously able to exploit to compromise remote systems.³⁴ As this example demonstrates, as soon as such exploits are made publicly or widely available, they can be patched and mitigated, removing their value as effective mechanisms for exploiting remote systems. BIS should therefore aim to maximize the ability of security researchers and professionals to publicly and widely share information and software, even when it may appear to encroach on the proposed controls. Unfortunately, the proposed implementation could hinder the sharing of this crucial information, because as BIS notes in its FAQ, exploit toolkits would potentially be classified under ECCN 4D004 if they are "specially designed" or modified for the generation of "Intrusion Software."³⁵

Decontrolling mass-market and publicly available tools would help alleviate some of the concerns surrounding the potential impact of the proposed implementation on security researchers and professionals, thereby forestalling the insecurity that would result from such individuals no longer having easy access to such tools.

Finally, the questions posed to BIS about the proposed rule's applicability to the exchange of exploit toolkits, amongst other challenges related to common security practices and software packages, demonstrate the ambiguity of the controls. Broadly decontrolling mass-market software and exchanges of technology will help

³⁴ See Dan Goodin, "Once again, Adobe releases emergency Flash patch for Hacking Team 0-days," *Ars Technica*, July 14, 2015, <http://arstechnica.com/security/2015/07/once-again-adobe-releases-emergency-flash-patch-for-hacking-team-0-days/>.

³⁵ BIS Intrusion and Surveillance Items FAQ #12.

BIS reduce classification requests, alleviate licensing burdens for incidentally controlled items, and allay some of the concerns of the security community.

B. Create a license exception or authorization for cybersecurity items that do not qualify for license exception TSU, but that are exported to non-government end users for defensive end uses

Certain cybersecurity items used for security research or network defense that are proprietary in nature, but do not qualify as mass-market software under license exception TSU, should merit decontrol if they are utilized for defensive purposes by non-state actors. Even with a broad license exception such as TSU in place, it is probable that some defensive security tools could be caught based on end user restrictions or restrictions imposed to limit access to only information security professionals. Nonetheless, defense-related sharing of cybersecurity items serves the public interest. We urge BIS to avoid subjecting researchers and vendors engaging in transfers for defensive purposes to an onerous licensing process in circumstances where license exception TSU does not apply. To address this, BIS should make available broad licenses to penetration testing products for extended periods of time for transfers involving non-governmental use and users where more permissive license exceptions are not available.

Examples of important defensive uses of cybersecurity items include exchanges of technology or software within corporate bug bounty programs, provision of internal access to cybersecurity items by a company or university to foreign nationals it employs or educates (which may qualify as a “deemed export”), and penetration testing services performed for non-governmental end users with the knowledge and consent of the owner or operator of that system. These uses all serve the public interest in enhancing digital security through defensive measures, and should therefore be protected.

Accordingly, a license exception or streamlined authorization process for cybersecurity items that are intended for a defensive, rather than offensive, end use should be available for exports to non-government end users. Such approach will require careful attention to end use and end user documentation requirements and evaluation processes. See section C.2 below for our recommendations on these issues.

We caution BIS against attempting to use export controls to regulate the entirety of digital threats posed by transnational criminal organizations or possible abuses of security testing or network defense systems. Such an endeavour would be inefficient and ineffective, and could come at the cost of undermining

cybersecurity priorities and stifling businesses that contribute to defensive activities. While penetration testing and network security tools have the capacity to be leveraged in an offensive manner, they represent a different class of products than single-purpose surveillance technologies. The U.S. government maintains alternative mechanisms for confronting criminal and economic threats online, and should seek recourse through more clear and directly applicable legal regimes when available and appropriate.³⁶

C. After adopting license exception TSU and broad license authorizations for non-governmental use and users, revise the licensing policy for remaining items to tailor it specifically to human rights concerns regarding cybersecurity items

As currently written the licensing policy of section 742.6(b)(5) is overbroad, ambiguous, difficult to properly implement, and insufficiently tailored to the specific human rights concerns that prompted the new controls. The problematic elements of the licensing policy language likely result from the breadth of items captured within the original proposed rule due to the rule's restriction on application of license exception TSU. If the TSU exception and related broad license authorizations for non-government use and users are adopted as we recommend, the licensing policy can be greatly streamlined and simplified.

While we are concerned about the implications of the proposed rules for fundamental information security practices, these concerns do not negate the history of abuse that inspired both of the proposed rules. We applaud the initiative of BIS in imposing an additional License Review Policy for Cybersecurity Items. The requirements of this policy, however, prioritize evaluative criteria that do not contribute to human rights objectives and may not be technically feasible. The Cybersecurity Items originally targeted by the Wassenaar Arrangement indeed warrant heightened scrutiny – such products are portable and once in place, they become a lasting mechanism of intrusive surveillance. There are ample cases of American-manufactured surveillance items, otherwise covered under encryption controls, being transhipped to sanctioned countries,³⁷ as well as examples of Intrusion Software developers claiming ignorance when their products have been used by foreign governments to spy on U.S. persons.³⁸ BIS should use the License Review Policy to refocus on preventing the transfer and transshipment of sensitive technologies in circumstances where they pose a risk to fundamental human rights

³⁶ For example, Executive Order 13694, mutual legal assistance treaty regimes, and/or domestic wiretapping statutes, as appropriate.

³⁷ Marquis-Boire et al., "Planet Blue Coat."

³⁸ "Hacking Team," Wikileaks, July 8, 2015, <https://www.wikileaks.org/hackingteam/emails/emailid/49683>.

and promoting greater accountability on the part of vendors to conduct due diligence on the end uses of the technology they are selling.

If BIS implements the license exception TSU and broad license authorizations for non-government use and users, as recommended above, decontrolling mass-market and dual-use items, it will limit the scope and types of items controlled under the rule in the first instance. In that case, we urge BIS to also adopt the following specific changes to the licensing policy.³⁹

1. *The significant human rights impact of the cybersecurity items of primary concern warrants stronger review policies that apply to known repressive regimes, as well as to end users elsewhere.*

Advanced surveillance tools designed for use by law enforcement agencies and government actors require strong, across-the-board oversight to prevent use of such tools in a manner that compromises internationally recognized human rights. A presumption of favorable treatment for exports of these powerful tools to any end user, even to allied states, discredits the United States' underlying commitment to human rights. Additionally, it is not sufficient to rely strictly on Country Groups, since these classifications have not traditionally been based on human rights considerations.⁴⁰ Several countries listed under Country Group B – such as Bahrain, Ethiopia and Morocco – have been accused of using FinFisher and Hacking Team products for compromising the communications of democracy activists, including individuals based in the United States.

This approach will also have the effect of simplifying the licensing policy, obviating the need for designation of actors for special treatment and subjective interpretations that could undermine the goal of the controls. In addition to the review policies we recommend later, a presumption of denial is appropriate when the end user has a track record of violating human rights or bears a transshipment risk, wherever located.

2. *Case-by-case licensing review should require, and carefully assess, details regarding end user and end use of the cybersecurity item.*

In conducting review of license applications, BIS, the Department of State, and others involved in the review process will need to evaluate the end user and probable end use of the cybersecurity item in order to determine its potential

³⁹ We note that these recommendations *only* apply if BIS applies the TSU License Exception or an equivalent carveout for mass market software and similar dual-use items.

⁴⁰ "License exceptions – Supplement No. 1 to Part 740," https://www.bis.doc.gov/index.php/forms-documents/doc_download/944-740-supp-1.

human rights impact. The proposed rule should incorporate the following changes to facilitate this evaluation.

First, to the extent that BIS will rely on the term “government end-user” in the rule (or references to the inverse circumstance, e.g., non-government end-user), the definition of “government end-user” in §772.1 requires revision to account for quasi-governmental, state-captured entities that may implement state policies on surveillance and censorship. Notably, the current definition explicitly excludes “utilities (including telecommunications companies and Internet service providers).” It is well-documented that many telecommunications companies and Internet service providers are closely tied to their home governments, and may deploy surveillance tools against users on behalf of the state, either willfully or by legal compulsion.⁴¹ To prevent artificial distinctions among end users, this exclusion within the definition should be removed, and the definition of governmental end-user broadened to include entities that are owned, operated, or otherwise subject to control by the state.

Second, the rule should reflect human rights-based due diligence requirements in §748.8(z), which lays out the unique application and submission requirements for cybersecurity items. While the EAR currently requires license applications to include identification of the actual end user and specific end use, BIS should request further details for cybersecurity items, given their demonstrated and repeated use to undermine human rights.

Previously, some of the Commenters had encouraged BIS to impose License Review Policies that:⁴²

- consider consultations and post-sales support requirements and infrastructure within Intrusion Software and IP Network Surveillance license applications, such as whether the device will be located in a national backbone and questions received by the client on the usage of the system;
- maintain technical expectations about how exempted systems should operate in order to achieve legitimate and narrowly-defined objectives in order to minimize the risk of relabelling; and

⁴¹ In both the Intrusion Software and the IP Network Surveillance cases, systems have been found embedded in the networks of telecommunications companies, compromising the traffic of Internet users; for example, the FinFisher infection proxies documented in Turkmentelecom. See “FinFisher: FinFly ISP Project, Turkmenistan,” available at <https://www.wikileaks.org/spyfiles/docs/GAMMA-2011-TMFinFinF-en.pdf>. In many countries of concern, legal requirements placed on telecommunications companies and ISPs to cooperate with surveillance do not adequately protect the right to privacy.

⁴² Anderson, “Considerations on the Wassenaar Arrangement Control List Additions for Surveillance Technologies.”

- review items not only based on their technical specification, but also their advertising material, integrations, partnerships, customers, passive operations, and end use.

Increased documentation requirements would allow for BIS to better account for differences between penetration testing tools and transfers of more sensitive technologies, while improving its overall ability to detect attempts to mischaracterize transfers. In addition to these characteristics, BIS could mandate disclosure of:

- whether the exporter maintains partnerships with Intrusion Software vendors;
- whether pertinent patents or sales material make reference to lawful interception or surveillance use cases;
- whether the system is sold as a package with Intrusion Software and whether any Intrusion Software product is reliant on the system or operation in question for operation;
- whether the product is primarily marketed to, or only sold to, law enforcement or intelligence agencies;
- whether the end recipient is a law enforcement or intelligence agency, or an entity with known relationships to such sectors;
- whether and how the vendor can account for changes in ownership or control of the item, as well as post-transfer control in the event of transshipment;
- whether the primary placement or capabilities of the device would enable its end recipient the ability to tamper with public access networks; and
- the actual network(s) on which the product is intended for deployment.

The disclosure of marketing material should be a primary component of any licensing policies for both controls. Intrusion Software and Network Surveillance systems marketed to law enforcement agencies and government actors bear striking differences from their commercial counterparts, not only in terms of support services, but also in sales material and accompanying product documentation. Moreover, these products are promoted within a broader, semi-open market for Intrusion Software systems, through tradeshows such as ISS World and Milipol.⁴³ The sales language and documentation offered to governmental customers will be necessarily distinct from that of defensive

⁴³ For more on these trade shows, see, e.g. “The Surveillance Catalog: Where governments get their tools,” The Wall Street Journal, February 7, 2012, <http://graphics.wsj.com/surveillance-catalog/attendees/>; Lisa Evans, “Surveillance trade shows: which government agencies attend?” The Guardian, February 7, 2012, <http://www.theguardian.com/news/datablog/2012/feb/07/surveillance-shows-attendees-iss-world>.

pentesting tools, based on prospective customer needs and product capabilities. Requesting such material can improve BIS's ability to incorporate human rights considerations in the course of licensing decisions, and further contribute to its ability to craft regulations that do not unnecessarily burden defensive products.

3. *Language providing for distinct treatment of “items that have or support rootkit or zero-day exploit capabilities” is unnecessary, may negatively constrain security research, and should be removed.*

The proposed rule has introduced new terminology – namely regarding rootkit or zero-day exploit capabilities – that is ambiguously understood within industry and undefined by BIS.⁴⁴ Given these ambiguities, this language should be removed. Similarly, language addressing rootkit or zero-days in “Unique application and submission requirements” and “Regional stability” licensing policies should also be removed.

As we understand, BIS's intention with these requirements is to identify the provision of high-end, pre-packaged exploits for embedding into Intrusion Software, often through subscription plans and designed for integration with a specific product. However, the publication or disclosure of security vulnerabilities frequently occurs through the release of a module for pentesting frameworks, in the same capacity that exploit brokers ship their product as modules for proprietary offensive systems.⁴⁵ As a result, it may not be possible or desirable for a product to systematically preclude support for zero-days or rootkits. Moreover, a case-by-case licensing review policy focused on end user and end use may prove more effective from a human rights standpoint than designating a subset of Intrusion Software for a presumption of denial. Instead, whether a vendor offers, or maintains partnerships with companies who do, exploit services may certainly be a characteristic germane to the license consideration process, if these terms are properly defined.

D. Provide guidance on the “generation” component of ECCN 4D004 to preclude certain classes of development tools

Common development and reverse engineering tools such as OllyDbg and Immunity Debugger present themselves as a “powerful new way to write exploits, analyze malware, and reverse engineer binary files.”⁴⁶ While BIS has clarified that general purpose development tools would not be controlled as software for the

⁴⁴ Allen Householder, “Like Nailing Jelly to the Wall: Difficulties in Defining ‘Zero-Day Exploit,’” *CERT/CC Blog*, July 7, 2015, <https://www.cert.org/blogs/certcc/post.cfm?EntryID=247>.

⁴⁵ “Hacking Team,” *Wikileaks*, July 8, 2015, <https://www.wikileaks.org/hackingteam/emails/emailid/49683>.

⁴⁶ See <http://www.immunityinc.com/products/debugger/>.

generation of Intrusion Software, these specific tools appear “peculiarly responsible” for the generation of Intrusion Software – while otherwise not constituting the command and delivery platforms or pentesting tools noted in Cybersecurity Items FAQ #29, nor necessarily including encryption.⁴⁷ Moreover, the controlled software and technologies are not subject to the exceptions offered in the definition of Intrusion Software for hypervisors, debuggers or Software Reverse Engineering.

While these tools could be employed for the generation of malware that is used for intelligence or criminal purposes, they represent a different class of products from applications such as FinFisher’s FinSpy Agent and Hacking Team’s RCS Console. The effective difference between these two classes of products is that FinSpy Agent and RCS Console are specially designed for integration and creation of a specific Intrusion Software product.

BIS should issue guidance that differentiates and decontrols security-focused reverse engineering and exploit development platforms from those tools that are offered for the creation of the specific Intrusion Software packages, such as RCS Console.

E. Narrowly define the proposed rules on “technology” related to Intrusion Software (4E001) to control government end users and end uses, or military purposes

BIS should formally clarify the scope of the 4E001 control on “development” of Intrusion Software and establish an explicit policy that decontrols common technology transfers, narrowing the controls so that they apply *only* to end use cases and end users facilitating or conducting surveillance. This would greatly reduce controversy within the security community regarding the proposal on technology for “development” of Intrusion Software. Furthermore, decontrolling the release of technology to non-governmental uses and users would substantially reduce the immediately obvious deemed export and intercompany transfers issues.

The omission of the standard “production” or “use” from the control, in addition to outreach from BIS since the release of the proposed rule, indicates that this control was designed to be narrow. However, ongoing attempts to describe a technical line between normal research and problematic transfers may prove to be insufficient to prevent a chilling effect stemming from confusion over where that line lies. As a result, mere guidance is not enough; instead, BIS should clearly narrow application

⁴⁷ BIS, “Intrusion and Surveillance Items,” <http://www.bis.doc.gov/index.php/policy-guidance/faqs>.

of the rule only to transfers for government end users and military or law enforcement end uses.

The Wassenaar Plenary's primary intention through 4E001.c appears to be control of commercial activities related to the preparation and integration of exploits into Intrusion Software and command and delivery platforms. In its FAQs, BIS had sought to clarify the scope of the technology for development for Intrusion Software through examples such as:

1. Information "required for" developing, testing, refining, and evaluating "Intrusion Software," in order, for example, technical data to create a controllable exploit that can reliably and predictably defeat protective countermeasures and extract information, and
2. Information on how to prepare the exploit for delivery or integrate it into a command and delivery platform.⁴⁸

BIS further attempts to constrain the scope of the control by noting that Intrusion Software only constitutes what it perceives as a narrow subset of malware and exploits.

This technology control can be understood as attempting to control a primary component of the close and continuing relationship between Intrusion Software vendors and clients employing exploits for the compromise of remote devices. The most visible vendor of such services is the French firm VUPEN Security, whose products and research enable intermediaries to better develop and deploy Intrusion Software through providing reliable exploits. In its trade literature, VUPEN notes that:

*Law enforcement agencies need the most advanced IT intrusion research and the most reliable attack tools to covertly and remotely gain access to computer systems. Using previously unknown software vulnerabilities and exploits which bypass Antivirus products and modern operating system protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) could help investigators to successfully achieve this task.*⁴⁹

⁴⁸ BIS Intrusion and Surveillance Items FAQ #4.

⁴⁹ "Exploits for Law Enforcement Agencies," VUPEN Security, available at https://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf.

As we understand these services are representative of the “proprietary research on the vulnerabilities and exploitation of computers and network-capable devices” that BIS describes in its “Scope of New Entries” and FAQ #4.⁵⁰

There is uniform agreement between civil society and industry that export controls should incentivize responsible disclosure of vulnerabilities through primary vendors, information security firms and intermediaries conducting bug bounties. However, it remains difficult to distinguish between this “white market” and problematic, “black market” vulnerability sales based on technical data transfers alone, since the difference is primarily based on contractual arrangements and buyer.⁵¹

As others have noted in specific discussions about the rules:

When a developer sells privileged vulnerability information they typically provide compilable source code and a document describing the vulnerability in full. This is essentially the same information that someone would submit to e.g. Microsoft Security when reporting a vulnerability: a writeup, and a PoC.⁵²

The publicly released vulnerability disclosures available through platforms and organizations such as HackerOne or the Zero Day Initiative reinforce that essential security reporting does not simply entail the release of a binary exploit, and requires complementary documentation and discussion.⁵³ Even further, the process of determining whether an exploit can be developed to “reliably and predictably defeat protective countermeasures and extract information” is frequently a pressing security question.⁵⁴

⁵⁰ According to the “Scope of New Entries” section of the rule proposed by BIS on May 20, 2015, “Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, Intrusion Software include network penetration testing products that use Intrusion Software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of Intrusion Software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices. The new entry on the CCL that would control Internet Protocol (IP) network communications surveillance systems or equipment is restricted to products that perform all of the functions listed; however, the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry;” BIS Intrusion and Surveillance Items FAQ #4.

⁵¹ Mailyn Fidler, “Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis,” April 2014, <http://moritzlaw.osu.edu/students/groups/is/files/2015/06/Fidler-Second-Review-Changes-Made.pdf>.

⁵² “On Definitions and Limits,” <https://lists.alchemistowl.org/pipermail/regs/2015-June/000249.html>.

⁵³ “XXS in Dropbox main domain,” <https://hackerone.com/reports/59356>.

⁵⁴ The Heartbleed vulnerability provides an illustrative example. Upon release of the vulnerability, there were open questions about whether the issue could be reliably employed to extract private keys from a remote system (qualifying under the Intrusion Software criteria). After an open challenge by Cloudflare and others, cooperation between private companies and researchers lead to the development of more reliable exploitation of the Heartbleed vulnerability. While this example would have been decontrolled by the General Technology

The challenges of establishing a strictly technical definition of problematic transfers were made more clear by the product information and communications between Hacking Team and exploit brokers, such as VUPEN and Netragard. These emails clearly demonstrate a private market for the sale of exploits to the highest bidder; however, the information shared with Hacking Team for marketing and sales of vulnerabilities by these vendors are not substantially different from the information disclosed in a critical vulnerability (CVE) report.⁵⁵

Beyond the inherent risks of overbreadth, the pursuit of a strictly technical line of difference between security research and exports of concern will limit the ultimate effectiveness of such control. The primary value provided by exploit brokers is information on the nature of a vulnerability – the proof of concept that BIS has repeatedly asserted is not controlled. In very few circumstances is more required to understand and replicate an attack than access to a proof of concept or working exploit. A proof of concept “shellcode” can be replaced by functional “shellcode” for the compromise of the device.⁵⁶ Permitting release of proof of concepts while controlling technical data on exploit techniques becomes a futile endeavour, as it will be easy to discern mechanisms from source code or decompiled binaries. In fact, much of the learning process occurs from reverse engineering of exploits found in the wild, even in the case of sophisticated Intrusion Software built by state actors.

Some elements of the security industry appear to be open to regulations that create clear and consistent expectations about responsible behavior. For example, Netragard has acknowledged that it was unaware of the end use and end users of its Exploit Acquisition Program, and publicly stated that the “zero-day exploit market needs to be thoughtfully regulated,” adding that:

[R]egulations should provide a framework for the legitimate sale of 0-day exploits. They should establish a set of guidelines to help control who can responsibly purchase 0-day exploits. Such regulations would make our jobs as ethical 0-day exploit brokers much easier and far less risky.⁵⁷

As with licensing policy, in considering end use and end users, strictly controlling against “military end use” or governmental users may not be sufficient. This

Note, this is representative of common practice that often is not public and may not be covered as fundamental research.

⁵⁵ “Hacking Team,” *Wikileaks*, July 8, 2015, <https://www.wikileaks.org/hackingteam/emails/emailid/49683>.

⁵⁶ Ivan Arce, “On the Quality of Exploit Code,” *RSA Conference 2005*, <http://www.coresecurity.com/system/files/HT2-301-IvanArce-v1.1.pdf>.

⁵⁷ Adriel Desautels, “The HackingTeam Breach & EAP,” *Netragard*, July 2015, <https://www.netragard.com/the-hackingteam-breach-eap>.

approach will pose a few challenges; namely in protecting disclosure to CERTs, other entities responsible for formal disclosure processes, or for government-provided services. This requires nuance, however, since such entities may also be compelled to disclose vulnerability information to intelligence agencies. This necessitates end use controls, in addition to end user limitations, due to the diverse ways that “government end user” might be too narrow.

F. Narrowly defined rules for technology necessitate clear “Know Your Customer” guidance

As with other industries, “Know Your Customer” policies are processes built around detecting and responding to a series of criteria (or “red flags”) that could indicate potentially suspicious transactions. The Department of Commerce is aware that sensitive technologies are often at risk for transshipment or illicit trade, and has a history of providing industry-specific guidance to exporters to address these types of concerns.⁵⁸ In the absence of clear guidance regarding the export surveillance technology – and as an attempt to promote industry self-regulation – civil society organizations and multi-stakeholder initiatives have offered their own recommendations, based on experiences and best practices, as well as international norms such as the UN Guiding Principles on Business & Human Rights.⁵⁹ Examples of detailed suggestions on developing a “Know Your Customer” regime appropriate for censorship and surveillance technologies have been documented by the Electronic Frontier Foundation and the Global Network Initiative, including recommendations on the scope and structure of the process and key definitions.⁶⁰

Given the narrow scope of the proposed Intrusion Software control, “Know Your Customer” guidelines and related due diligence are critical to ensure that the rule still has the intended effect of preventing the transfer of technology that can be used to facilitate human rights abuses. At a minimum, in evaluating whether a technology may be used for repressive purposes, companies, organizations or individuals should assess the likely end use and end user of a product with reasonable certainty. These processes should include providing documentation

⁵⁸ See “Know Your Customer Guidance,” U.S. Department of Commerce’s Bureau of Industry and Security, <https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/freight-forwarder-guidance/23-compliance-a-training/47-know-your-customer-guidance>.

⁵⁹ UN, “Guiding Principles on Business and Human Rights,” 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

⁶⁰ Cindy Cohn and Jillian C. York, “‘Know Your Customer’ Standards for Sales of Surveillance Equipment,” The Electronic Frontier Foundation, October 24, 2011, <https://www.eff.org/deeplinks/2011/10/it%E2%80%99s-time-know-your-customer-standards-sales-surveillance-equipment>; Cindy Cohn, Trevor Timm, and Jillian C. York, “Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes,” Electronic Frontier Foundation, April 2012, <https://www.eff.org/document/human-rights-and-technology-sales>.

describing the nature of the due diligence conducted and responses from the end recipient.

Such documentation may include, but is not limited to:

- Relationship with the contracting entity, including length of relationship, contractual mechanisms for compliance, and demonstrated history of compliance with contractual and legal obligations;
- Final country destination, recipient, and end use of the technology, such as location in a network or nature of the buyer, supported by clear and detailed documentation;
- Extent of ongoing servicing of the technology, including potential for post-export checks on compliance; and
- Design of the technology and customizations.

To aid in compliance with these requirements, the Department of Commerce should provide specific lists of possible red flags that illustrate the type of circumstances that should cause reasonable suspicion that a transaction will violate the new controls for cybersecurity items.

Relevant red flags may include:

- Originating IP addresses for software updates or other forms of communications, which may indicate that a product has been transferred or resold to another entity;
- Language requirements and device support requests;
- Provision of equipment that vastly exceed the traffic requirements for the stated installation location; and
- Qualifications and background of participants present at training sessions.

The Commerce Department should emphasize that “Know your Customer” encompasses “know your reseller” and “know your regional partners,” which will help mitigate the risk that companies attempt to “self-blind” by ignoring public research, records on the location of service and update requests, and indications of the actual end uses reflected by customers’ requests. The activities of FinFisher and Hacking Team demonstrate that companies have had little incentive in the past to perform due diligence or respond to reports of abuse, creating a “race to the bottom” that disincentivizes better behavior in the broader industry. It is not sufficient for a company to perform “Know Your Customer” checks without taking reasonable steps to determine whether the technology in question is likely to be

transferred from the original customer to end users in repressive countries who may use it for nefarious purposes.

The Commerce Department should also consult with industry and civil society to promote implementation of “Know Your Customer” policies that will reduce the potential for approved exports to be misappropriated for the abuse of human rights. Recurring outreach will also help ensure that the Commerce Department’s efforts match the fast pace of technological development and also address evolving ways in which infringing parties may attempt to bypass the controls.

G. Issue clear guidance on key terminology introduced into the text of the rule

In order to minimize ambiguity and clarify enforcement objectives, BIS should issue clear definitions regarding the terminology used in future proposed and final rules. Currently, the proposed rule uses a number of terms of art that are either poorly defined or not defined at all. Adding to the confusion, many of these terms lack widely-agreed upon definitions in the technical community. Such terms must either be clearly defined, or removed from the text of the proposed rule.

As noted previously, our concerns include the use of the terms “rootkit” and “zero-day exploit capabilities” found in the License Review Policy for Cybersecurity Items section of the draft rule and the proposed additions to 15 CFR 742.6.⁶¹ Both of these terms are undefined by BIS and have no agreed-upon definition in the technical community.⁶² Furthermore, as BIS has acknowledged, some of the terms or functions included in ECCN’s 5A001.j definition are not defined, including “carrier class IP network,” “indexing of extracted data,” and the basis of the “relational network” mapping within the control. BIS should explicitly define these terms – and where appropriate provide examples of their meaning – in any final rule that it issues.

Failing to define such terms will result in a rule that has an unnecessary chilling effect on good faith security research because of ambiguity about what can and what cannot be legally exported. We have already seen the detrimental result of poorly-defined terminology on the security research community in other areas of U.S. law, and urge BIS to avoid making the same mistakes in this proposed rule.⁶³

⁶¹ 80 FR 28853. “License Review Policy for Cybersecurity Items”; 80 FR 28853. “§ 742.6 Regional stability.”

⁶² For example, some in the community define the term “zero-day” to refer to any vulnerability that has not been publicly released. Other use the term to refer to any unpatched vulnerability. Likewise, the term “rootkit” has a range of meanings, from special software installed at the firmware level to manipulate a normally installed operating system. Other use the term to refer to any software that tries to mask its existence from the user.

⁶³ For example, the ambiguities surrounding the rights of security researchers under Section 1201 of the Digital Millennium Copyright Act (17 USC 1201) continue to stymie good faith research and force researchers to seek

Clear definitions of key terms would also provide for the basis of a better understanding and more efficient uses of the license exceptions proposed previously.

Given the complexity of the rule, we similarly urge BIS to include language in its “Scope of the New Entries” section explicitly noting the forms of security research (both public and proprietary) that are outside the scope of the controls. Specific examples of controlled or decontrolled products or software would be welcome and would assist the software development and security communities – whose members are generally unfamiliar with the nuances of export controls – in properly interpreting the proposed rule.

H. Issue an amended version of the proposed rule on Intrusion Software prior to publication of the final rule

We appreciate BIS’s initiative in publishing the proposed rule and requesting comments, and its willingness to provide opportunities for clarifications on the language. The open and iterative process that public comments enable lead to better rules, and have already had a demonstrable impact by avoiding the numerous issues that would have arisen had BIS simply published a final rule without first seeking input from the public. In light of the numerous concerns outlined in these comments, and the significant revisions that addressing them will likely entail, we request that BIS amend the proposed rules and issue a second request for comments prior to publishing a final rule. We note that this is not a request to extend the current comment period, nor do we believe that BIS will be unable to resolve the issues that we have noted within the constraints of the language that the United States has committed to implement as a Wassenaar member. Instead, issuing a revised draft rule and seeking additional comments will simply ensure that the concerns that commenters have outlined have been adequately and appropriately addressed prior to publication of a final rule. This second proposed rule should include specific information on license exceptions and definitions of key terms, which were omitted from the first proposed rule, in order to allow affected communities and industries to fully assess the impact of the rules on their commercial operations and articulate their concerns through public comment.

changes to the law; see Copyright Office Hearing on “Library of Congress Sixth Triennial Rulemaking: Class 25,” May 26, 2015.

I. Establish an iterative process to see how the rule evolves in implementation

Public debates about the role of regulation in impeding the proliferation of surveillance and censorship equipment have often hinged on whether export control agencies are responsive enough to adapt to changes in technology and industry norms. While these controls are intended to define single-purpose surveillance products, rather than dual-use technologies such as deep packet inspection equipment, the subsequent reaction to BIS's proposed rules demonstrates an increased need for continued consultations between government agencies and representatives from industry, technical communities, academia and civil society. Over time, changes in cybersecurity technology may warrant additional license exceptions – or even narrowing of licenses – for these rules, as well as for encryption and communication intercepting devices controls.

As an example, it may be necessary in the future to add Network Intrusion Detection to the excluded design purposes under the IP Network Surveillance systems control. Network intrusion detection systems, such as Bro, Snort, and other commercial products, are becoming increasingly critical for maintaining the security of modern networks. While we do not feel that such tools as currently crafted will be subject to the proposed 5A001.j rules, it is possible that future advances in technology might create ambiguities about whether or not they are controlled. For the purpose of this comment period, ensuring that the new categories are subject to the TSU and clarifying the definition of some of the terms of art discussed previously will help alleviate these concerns, but in the long-term ongoing consultations to ensure that the controls continue to be appropriately tailored as the technology evolves will likely be necessary.

V. Conclusion

We would like to reiterate our gratitude to the Bureau of Industry and Security for publishing the proposed rule for comment and for considering the recommendations submitted here. We hope that we have offered insight that will lead to a final rule that addresses the human rights concerns posed by the spread of the single-use surveillance technologies without adversely affecting a variety of additional technologies, including important security research tools.

We continue to believe that it is possible to implement the 2013 Wassenaar controls related to surveillance technology in a timely manner that balances both the human rights concerns that prompted these controls and the important goal of preventing security researchers and professionals from being subject to overbroad restrictions

that could have a chilling effect on their activities. In order to achieve that balance, we urge the Commerce Department to carefully consider draft language and continue to consult with a broad range of civil society, academic experts, and security professionals to ensure that unintended consequences are mitigated to the greatest extent possible without sacrificing the important policy goals advanced by the original rules.

In the event that a final rule threatens to be either overinclusive or underinclusive in the technologies that it controls, we believe that it is better to err on the side of underinclusion, potentially excluding some surveillance technologies that might warrant control but can be addressed using other policy options besides export controls. BIS can revisit the controls in the future if they need to be amended. However, we are optimistic that it is possible to strike the right balance and look forward to working with the Commerce Department to achieve that goal.

Thank you for your consideration.

Respectfully submitted,

Access

Center for Democracy & Technology

Collin Anderson

Electronic Frontier Foundation

Human Rights Watch

New America's Open Technology Institute

PUBLIC SUBMISSION

As of: 7/29/15 6:43 PM
Received: July 29, 2015
Status: Posted
Posted: July 29, 2015
Tracking No. 1jz-8k9a-9u9b
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0266

Boeing Comments BIS WA Intrusion 7-29

Submitter Information

General Comment

See attached

Attachments

Boeing Comments BIS WA Intrusion 7-29



July 20, 2015

Ms. Catherine Wheeler, Director
Information Control Technology Division
Bureau of Industry and Security
Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

**Subject: RIN 0694-AG49, Wassenaar Arrangement 2013 Plenary Agreements
Implementation: Intrusion and Surveillance Items**

**Reference: Federal Register/ Vol. 80, No. 97/ Wednesday, May 20, 2015/ Proposed
Rules**

Dear Ms. Wheeler,

The Boeing Company (“Boeing”) appreciates the opportunity to provide comments to the Bureau of Industry and Security (“BIS”) on the Proposed Rule for implementing new controls on certain cybersecurity items in accordance with the Wassenaar Arrangement Plenary meeting in December 2013. Boeing develops and utilizes items that would be captured by the proposed controls. Our comments cover three broad areas: scope of controls in the proposed rule; potential control of network protection software; and the separate regulatory processes for encryption and cybersecurity items when present in a single product.

The overall scope of the controls set forth in the Proposed Rule appears broader than what was subsequently published in the Frequently Asked Questions (“FAQs”) and discussed in the BIS teleconference on this topic. For example, it is unclear whether the proposal would control only software and related items that penetrate a network and insert software that causes the network to operate contrary to its intended design, or whether the proposal also would control the types of products that companies routinely use to test and address potential vulnerabilities in their networks. Boeing recommends that BIS refine the proposed control text to align with information in the FAQs and the issues raised in the teleconference through a second Proposed Rule for public comment.

Secondly, a significant concern for Boeing is the potential to establish burdensome controls on network protection products from vendors such as *Hewlett Packard*, *Cisco Systems*, and *McAfee*, which the company uses in a variety of scenarios:

- Boeing uses penetration-testing products to analyze the security of our data and business networks both in the United States and in our non-U.S. subsidiaries;
- Boeing collaborates on network protection with suppliers (whom we carefully evaluate, screen, and monitor) that receive both U.S. Government and Boeing proprietary technology;
- Boeing works with network protection suppliers to improve their products for use in our business and research environments; and
- Boeing's Electronic & Information Solutions division develops network protection products to help customers protect their data, secure their command, control and communications networks and systems, and operate effectively in the cyber domain.

Boeing recommends that the network protection activities described above remain unburdened from restrictions that are intended for malicious uses of cybersecurity items.

Finally, the proposed addition in Part 748 Supplement 2 indicates that separate processes are required for encryption elements and for cybersecurity elements that are often present in the same product. For example, Supplement 2 paragraph (r) sets forth processes for cryptography in Category 5 items. A new paragraph (z) proposes new processes that must be met "separately" for cybersecurity features in Category 4 items. Boeing recommends establishing one set of requirements and processes that would enable exporters to provide cybersecurity and encryption information at the same time.

Thank you for the opportunity to provide comments. Please do not hesitate to contact me if you have any questions or need additional information. I can be reached at 703-465-3505 or via email at christopher.e.haave@boeing.com.

Sincerely,

A handwritten signature in cursive script, appearing to read "Christopher Haave".

Christopher Haave
Director, Global Trade Controls

PUBLIC SUBMISSION

As of: 7/30/15 11:21 AM
Received: July 30, 2015
Status: Posted
Posted: July 30, 2015
Tracking No. 1jz-8k9r-d7b8
Comments Due: July 20, 2015
Submission Type: Unknown

Docket: BIS-2015-0011

Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Comment On: BIS-2015-0011-0001

Wassenaar Arrangement Plenary Agreements Implementation; Intrusion and Surveillance Items

Document: BIS-2015-0011-0267

Michael Angelo

Submitter Information

General Comment

See Attached

Attachments

Michael Angelo

Sharron Cook

From: Michael F. Angelo <mfa@peoplepc.com>
Sent: Monday, April 13, 2015 5:21 PM
To: Sharron Cook
Subject: RE: RIN 0694-AG49

Sorry, The bolding disappeared. :-(

I am concerned about capturing penetration testing software as well as security analysis tools.

I am concerned about IP surveillance systems being caught, as the distinction between sniffers in the documents are vague. (ie. This would capture Wireshark and other software).

I am also concerned about forcing an interaction between Industry and DHS for the communication of computer security vulnerabilities. The president said it would be voluntary, however this rule would make it anything but voluntary and would disable the already existing channels in place today.

Michael F. Angelo, CRISC, CISSP
16118 Lafone Dr | Spring, TX 77379
713-822-3014 / mfa@peoplepc.com

The best way to predict the future is to invent it -- Alan Kay
This email (including all attachments) may contain material that is confidential, privileged or attorney work product, and is provided for the sole use of the intended recipient. Any review, use, copying or distribution by anyone other than the intended recipient is strictly prohibited. If you are not the intended recipient, please contact me immediately and delete all copies of this email (and all attachments).

-----Original Message-----

From: Sharron Cook [mailto:Sharron.Cook@bis.doc.gov]
Sent: Monday, April 13, 2015 11:15 AM
To: Michael F. Angelo
Subject: RE: RIN 0694-AG49

So you are worried about this part ... " the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry. "

-----Original Message-----

From: Michael F. Angelo [mailto:mfa@peoplepc.com]
Sent: Monday, April 13, 2015 12:10 PM
To: Sharron Cook
Subject: RE: RIN 0694-AG49

Hi Sharron,

Below is a sample of what I am talking about.

Scope of the New Entries

Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices. The new entry on the CCL that would control Internet Protocol (IP) network communications surveillance systems or equipment is restricted to products that perform all of the functions listed; however, the Export Administration Regulations (EAR) also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry.

Ps. As an FYI the exemption for GOV is not really helpful. Most of the legitimate researchers finding and reporting vulnerabilities go through the already existing mechanisms (i.e. not US govt) .

Michael F. Angelo, CRISC, CISSP

16118 Lafone Dr | Spring, TX 77379

713-822-3014 / mfa@peoplepc.com

The best way to predict the future is to invent it -- Alan Kay

This email (including all attachments) may contain material that is confidential, privileged or attorney work product, and is provided for the sole use of the intended recipient. Any review, use, copying or distribution by anyone other than the intended recipient is strictly prohibited. If you are not the intended recipient, please contact me immediately and delete all copies of this email (and all attachments).

-----Original Message-----

From: Sharron Cook [mailto:Sharron.Cook@bis.doc.gov]
Sent: Monday, April 13, 2015 7:34 AM
To: Michael F. Angelo
Subject: RE: RIN 0694-AG49

I don't understand what you mean by "extensions." Please explain.

-----Original Message-----

From: Michael F. Angelo [mailto:mfa@peoplepc.com <mailto:mfa@peoplepc.com>]
Sent: Monday, April 13, 2015 8:32 AM
To: Sharron Cook
Subject: RE: RIN 0694-AG49

Thanks Sharron...

I am very concerned about the extensions in the implementation of the Wassenaar Cyber control. The ISTAC explicitly discussed the potential impact to industry of such extensions. Given our concerns, we were very careful in our response to the draft and attempted to protect against the over control and subsequent negative impact on US business. Our concern was that the Cyber controls would be extended as described in this document and that would stop US technology development and inhibit US industry to configure, defend, analyze, and mitigate issues in regional as well as multinational corporate security environments. In short the described Cyber implementation was what we were trying to avoid. :(Hopefully it is not too late to rethink this strategy and have a dialog before we go to far down this path.

Michael F. Angelo, CRISC, CISSP

16118 Lafone Dr | Spring, TX 77379

713-822-3014 / mfa@peoplepc.com <mailto:mfa@peoplepc.com>

The best way to predict the future is to invent it -- Alan Kay This email (including all attachments) may contain material that is confidential, privileged or attorney work product, and is provided for the sole use of the intended recipient. Any review, use, copying or distribution by anyone other than the intended recipient is strictly prohibited. If you are not the intended recipient, please contact me immediately and delete all copies of this email (and all attachments).

-----Original Message-----

From: Sharron Cook [mailto:Sharron.Cook@bis.doc.gov <mailto:Sharron.Cook@bis.doc.gov>]

Sent: Monday, April 13, 2015 7:01 AM

To: Michael F. Angelo

Subject: RE: RIN 0694-AG49

Not yet. Michael, your comments are welcome at any time.

-----Original Message-----

From: Michael F. Angelo [mailto:mfa@peoplepc.com <mailto:mfa@peoplepc.com>]

Sent: Sunday, April 12, 2015 4:52 PM

To: Sharron Cook

Subject: RIN 0694-AG49

Hi Sharron,

My name is Michael F. Angelo (on the BIS ISTAC), as part of my support for the TAC I was forwarded a copy of the above to referenced item to review. I understand I can submit official comments after it is published in the

federal register. Given that there are numerous elements of this Implementation Plan (which are extensions to the scope and plan of the original Wassenaar control) that will negatively impact US industry and commercial capability, I wanted to make sure I was in a position to comment as soon as it is officially published. Hence I was curious if there was an official publication date scheduled for it.

Michael F. Angelo, CRISC, CISSP

16118 Lafone Dr | Spring, TX 77379

713-822-3014 / mfa@peoplepc.com <mailto:mfa@peoplepc.com>
<mailto:mfa@peoplepc.com <mailto:mfa@peoplepc.com> >

Any sufficiently advanced technology is indistinguishable from magic --
Arthur C. Clarke

This email (including all attachments) may contain material that is confidential, privileged or attorney work product, and is provided for the sole use of the intended recipient. Any review, use, copying or distribution by anyone other than the intended recipient is strictly prohibited. If you are not the intended recipient, please contact me immediately and delete all copies of this email (and all attachments).