



**OPENING STATEMENT**

January 12, 2016

**MEDIA CONTACTS**

Susan Phalen, Matthew Ballard

**Statement of Committee Chairman Michael McCaul (R-TX)  
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee  
House Homeland Security Committee**

*Wassenaar: Cybersecurity & Export Control*

Remarks as Prepared

I appreciate the Gentlemen from Texas, Mr. Ratcliffe and Mr. Hurd, for having a hearing today on this very serious and consequential issue. Strengthening our nation's cybersecurity is of the utmost importance right now and will determine our Nation's position as a world leader in the future. The playing field for international conflict is constantly evolving. Cyber attacks can come from anywhere at any time, without any prior notification. As Chairman of the Homeland Security Committee, keeping Americans safe is my primary concern – and that is no simple task in such a dynamic environment. Unfortunately, the amendment to the Wassenaar Arrangement would depreciate the research, development, and deployment of important tools that we all use every day to secure against cyber attacks.

The United States has a duty to be a world leader. The establishment of a multilateral Arrangement to restrict the trade of conventional arms and dual-use goods and technologies has only been possible through strong American leadership. To continue fulfilling this imperative role, the United States must ensure that such agreements support technically and practically intelligent policies on cybersecurity.

If the matter at hand was simply a question of efficacy, we wouldn't be here today. If the only concern was that the Wassenaar Arrangement might have room for improvement, this conversation would be very different. But what has been violated here is the fundamental adage of "do no harm". The State Department agreed to an Arrangement that would restrict a broad group of information security tools and products. This agreement and the proposed implementation could hobble the entire cybersecurity ecosystem, as well as the cross-border data flows and global collaboration that support it. Weakening our cyber researchers and innovative service providers is bad enough, but as we've seen again and again, any weakness in our cyber posture will percolate to other industries and harm individual Americans.

Furthermore, under the Arrangement participating states already exchange specific information on a regular basis about global transfers of certain goods and technologies. Part of the Wassenaar Arrangement is looking at that information to find dubious acquisition trends. I don't see any limitation on the ability of the Wassenaar Arrangement to pursue the stated goals of increased transparency without adding burdensome and counterproductive licensing requirements. I hope the witnesses are

able to speak today about why the addition of intrusion software language to the Arrangement was preferred as the best means of achieving American goals instead of other options such as through sanctions, which would address bad actors more directly without the unintended consequences.

Last, the Homeland Security Committee worked hard in putting together and shaping information sharing legislation which was signed into law in December. That legislation facilitates the sharing of cyber information between the Federal Government and the private sector to assist security experts and others in rapidly identifying and resolving vulnerabilities that threaten the security of our networks. We must not backtrack on this progress. It is a priority of the Homeland Security Committee to investigate whether the domestic execution of the relevant cybersecurity section of the Wassenaar Arrangement would obstruct positive collaboration on cybersecurity that protects American information and information systems.

I hope the backlash received and the response here in Congress will prevent the State Department from attempting to take momentous negotiations upon themselves without consultation from stakeholders in the future. The Administration must not ignore the serious, broad implications of the results. What we won't stand for is de facto regulation of a thriving sector and cornerstone of American industry - An industry that provides the tools that we all, including governments, use to secure ourselves.

I expect the hearing today will send an important message that the intrusion software language in the Wassenaar Arrangement is simply unworkable. We in Congress expect that the Administration will work to correct these serious issues going forward.

###



**OPENING STATEMENT**

January 12, 2016

**MEDIA CONTACTS**

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman John Ratcliffe (R-TX)  
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee  
House Homeland Security Committee**

*Wassenaar: Cybersecurity & Export Control*

Remarks as Prepared

The House Homeland Security Committee Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies and the House Oversight and Government Reform Subcommittee on Information Technology meet today to hear from key industry and government stakeholders about the impact the Wassenaar Arrangement will have on the American people, U.S. businesses, and the cybersecurity industry.

First, I want to thank my friend Mr. Will Hurd, the gentleman from Texas, for co-chairing this hearing. Today we are doing what Americans would like to see more of in Congress. Two Committees that don't often get to work this closely are able to – and happy to – come together to tackle an issue that is extremely relevant to national security and the security of individuals' personal information. I believe this is one of our core duties in Congress: to bypass jurisdictional roadblocks and make real progress towards keeping our citizens safe.

Private industry in America is excellent at responding to consumer demands. Many companies, some here today, pride themselves on guaranteeing the security of their customers' personal information. Others represented here exist solely to help in securing that information. They also secure vital sectors of society, such as critical infrastructure and the financial sector. Their success hinges, in large part, on their ability to guarantee their own security.

Today, I hope to hear from our witnesses on how the Wassenaar Arrangement and its implementation would affect these objectives.

The Wassenaar Arrangement was established 20 years ago to apply to conventional arms and dual-use goods and technology. Changes made in 2013 sought to extend export controls to cybersecurity intrusion and surveillance software and technology. These changes were motivated by a desire to prevent authoritative regimes from repressing their people.

This intent is noble. Yet the Administration's implementation effort resulted in united dissent from the technology and cybersecurity industries, academics, and researchers. The energy and financial sectors voiced deep concerns. And they were echoed by civil society groups, who said the proposal could make communicating about security vulnerabilities almost impossible in certain cases.

The federal government engages in countless ways with the American people and our international partners. When proposing actions, the government should – at a minimum – do no harm to its own people.

I am interested to hear from our government witnesses how they believe this arrangement will successfully deter the accumulation of digital weapons, which aren't constructed in factories, don't need physical space for storage, and don't depend on traceable means of transport. I hope to better understand how they believe this export control framework can be effectively applied to intrusion software.

I agree that we should strive to limit dangerous technologies from falling into the hands of bad actors. But national security and Americans' personal security can't be sacrificed. There are many ways the United States strives to combat human rights violators and I hope to hear today about why this route was chosen over other options.

As we can see by the variety and size of the witness panel, the Wassenaar Arrangement has broad implications. Recent reports and the witness testimony today demonstrate that we are far from a consensus on this issue.

The Administration's top three cybersecurity priorities include 1) "protecting the country's critical infrastructure from cyber threats"; 2) "improving our ability to identify and report cyber incidents"; and 3) "engaging with international partners to promote internet freedom and build support for an open, interoperable, secure, and reliable cyberspace." I assume that our government witnesses are well versed in these goals and their prioritization.

Yet in reading comments to the proposed rule and general thoughts on the cybersecurity section of the Wassenaar Arrangement, one sees a probable contradiction of the first two goals. Additionally, it is unlikely that this Arrangement achieves the open and interoperable cyberspace that is in the public's interest. If we are to expect the cybersecurity provisions of this Arrangement to be workable, we need to make sure our stated intentions and actions are not contradictory. If we can't do that, I question why we as a country are agreeing to this updated Arrangement.

Just last month, Congress passed legislation to encourage the sharing of cyber threat information. Both the private sector and the government stand to benefit from the increased flow of valuable cyber threat information. Today, we need to hear whether the Wassenaar Arrangement would have a counterproductive impact on such sharing and whether it would undermine the law that the President just signed.

As a Nation, we advocate for human rights and assist those harmed by authoritarian regimes. However, we must first and foremost safeguard the security of our Nation and our citizens. I look forward to hearing from the witnesses about the path forward and how we can come together to best protect the American people.

###

Testimony of

Dr. Phyllis Schneck  
Deputy Under Secretary for Cybersecurity and Communications  
National Protection and Programs Directorate  
United States Department of Homeland Security

Before the  
United States House of Representatives  
Committee on Oversight and Government Reform  
And the  
Committee on Homeland Security

January 12, 2016

## **Introduction**

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, and Ranking Member Richmond and distinguished members of the Committees, let me begin by thanking you for the unwavering support provided to the Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD). We look forward to continuing to work with you in the coming year to ensure a homeland that is safe, secure, and resilient against terrorism, cyber-attacks, natural disasters, and other risks.

In particular, we appreciate Congress' efforts in passing the Cybersecurity Act of 2015 last month. This invaluable legislation will significantly enhance our ability to exchange cybersecurity threat information between the government and the private sector and will improve our ability to protect federal civilian networks.

NPPD undertakes its cybersecurity activities within its overarching mission to secure and enhance the resilience of the Nation's cyber and physical infrastructure. We view ourselves as a customer service organization, and our customers are federal civilian departments and agencies, state, local, tribal, and territorial governments, and the private sector. NPPD strives to

understand the mission, interests and equities of all of our customers to build trusted relationships for knowledge exchange and to better enable their resilience by creating and offering the right services and capabilities.

Within the private sector, NPPD maintains a particularly close partnership with the cybersecurity community – developers, vendors, and researchers that create the innovative solutions to help protect our Nation from cybersecurity risk. It is in this context that we consider the 2013 Wassenaar Agreement on Intrusion and Surveillance Items. I appreciate the concerns raised by many Members of Congress.

By way of background, the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multi-lateral forum intended to promote transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies. In 2013, Participating States to the WA agreed upon a new export control for “systems,” “equipment,” or “components” thereof, “specially designed” or modified for the generation, operation or delivery of, or communication with, “Intrusion Software.” Pursuant to this unanimous agreement, the Department of Commerce engaged in a rulemaking process as the U.S. Government’s lead for domestic implementation of WA rules. Industry feedback to a Notice of Proposed Rulemaking (NPRM) was overwhelmingly negative and raised significant concerns regarding implications for cybersecurity innovation, research, and information sharing.

NPPD and the DHS Science and Technology Directorate, the Department’s export control lead, have further consulted with numerous industry groups and solicited feedback through the Sector Coordinating Councils. For context, Sector Coordinating Councils are structures of the National Infrastructure Protection Plan Framework that bring together executives in the private sector to collaborate with each other and with the U.S. Government on key issues of cyber and infrastructure protection, transcending the competitive boundaries that traditionally block this type of collaboration within a sector. Most of our critical infrastructure sectors have a Sector Coordinating Council. It is important to note that the private sector participants expend great energy, resources and intellectual capital in these Sector Coordinating Councils, because they

know that the government strongly considers the resulting sector views in future planning and policymaking.

DHS understands that there are national security concerns that led to the development of this control with the aim to restrict exports of such tools related to intrusion software so they cannot be used maliciously. However, we need to ensure that in implementing the 2013 control, the U.S. does not inadvertently create greater problems and more risks than the security concerns that the control was intended to address. The interagency, including DHS, shall consider carefully the concerns raised by U.S. industry and legitimate potential impacts on the Nation's cybersecurity.

As the Committee knows, cybersecurity is defined by rapid change. Technology is evolving at a faster pace than ever before. Our adversaries are also changing rapidly, and are constantly developing new tools and attacks to compromise critical networks, steal data, and potentially damage our physical infrastructure. In this environment, it is essential for cybersecurity researchers and developers to share information rapidly across borders in the interest of creating the next security solution or combating an emerging risk.

For example, national cybersecurity response teams (such as Computer Security Incident Response Teams (CSIRTs)) rely on timely and actionable information about cybersecurity threats and vulnerabilities from researchers and other independent experts. In the United States, our CSIRT resides within NPPD, and is called the United States Computer Emergency Readiness Team (US-CERT). US-CERT relies upon international counterparts on a daily basis to help identify, respond to, and mitigate cybersecurity risks that threaten government and critical infrastructure networks. A substantial portion of information sharing with cybersecurity researchers occurs across national borders and this needs to be taken into account in implementing export controls.

Finally, there is a critical need for increased and sustained investment in cybersecurity research and development, rather than less. In crafting our approach to implementing the Wassenaar control, we need to take this into account, as well as the uncertainty expressed by many cybersecurity firms regarding the specific types of information that can be shared with their foreign-based subsidiaries, or with their own foreign national employees within the United States, without a license.

Evolving and sophisticated cyber threats pose a considerable challenge to securing critical infrastructure and government systems. As such, governments should implement policies to incentivize innovative research in measurably effective cybersecurity.

The United States is fortunate to have many global leaders in cybersecurity research and innovation within our borders. We also need to ensure that implementation of the Wassenaar control does not unduly disadvantage these companies in a global competition with their international peers.

Of course, NPPD is fully conscious of the significant risks posed by certain surveillance tools and intrusion software. There are myriad examples of governments using such tools to spy on dissidents, constrain freedom of expression, and engage in extrajudicial monitoring. But such examples also exemplify why we must support improved cybersecurity. We need a balanced approach that both protects cybersecurity research and innovation and make it harder for authoritarian governments to monitor dissidents or for cyber criminals to steal data about U.S. citizens. The inherent nature of many “cyber technologies” is that they are technologically agnostic; that is, the same software that is used to test a company’s cybersecurity can be used to conduct unauthorized or illegal surveillance. This demonstrates the complexity of the issue, and why further discussion is needed.

The Wassenaar Agreement on Intrusion and Surveillance Items was developed in response to a legitimate concern: reducing the proliferation of dual-use technologies that are used for malicious surveillance or hacking. But in implementing that control we need to avoid unintended consequences on cybersecurity. In a threat environment where our adversaries continue to gain in sophistication, we cannot afford to unduly constrain development of the next generation of cybersecurity solutions. Cybersecurity developers and vendors must be able to share information for legitimate purposes as quickly as possible. Researchers must be able to share appropriately vulnerability and threat information with US-CERT and national CSIRTs in friendly states. The interagency continues to consider the issue. In the meantime, DHS will continue to support national security efforts undertaken at the Wassenaar Arrangement while continuing to work with our interagency partners to strengthen U.S. cybersecurity.



**Written Testimony of**

**Dean C. Garfield  
President & CEO, Information Technology Industry Council  
(ITI)**

**Before the**

**Subcommittee on Information Technology  
Committee on Oversight and Government Reform**

**And**

**Subcommittee on Cybersecurity, Infrastructure Protection,  
and Security Technologies  
Committee on Homeland Security**

**U.S. House of Representatives**

***Wassenaar: Cybersecurity and Export Control***

**January 12, 2016**



**Written Testimony of  
Dean C. Garfield  
President & CEO, Information Technology Industry Council (ITI)**

**Before the  
Subcommittee on Information Technology  
Committee on Oversight and Government Reform**

**And**

**Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies  
Committee on Homeland Security  
U.S. House of Representatives**

*Wassenaar: Cybersecurity and Export Control*

**January 12, 2016**

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond, and members of the subcommittees, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before your subcommittees today on the important topic of the Wassenaar Arrangement and the implications for cybersecurity of imposing stricter export controls pursuant to 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 (the "Proposed Rule").<sup>1</sup> While we strongly support the Wassenaar Arrangement's human rights objectives of addressing the export and proliferation of weaponized malicious software, we have significant concerns regarding the commercial and security implications of this proposed means of achieving them. We welcome your interest and engagement on this subject.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity is critical to our members' success—the protection of our customers, our brands, and our intellectual property is an essential component of our business, and affects our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business in countries

---

<sup>1</sup> Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853 (proposed May 20, 2015), available at <https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>.



around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries across the globe, servicing customers that typically span the full range of global industry sectors, such as banking and energy. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

I will focus my testimony on four areas: (1) The critical importance of cross-border data flows to cybersecurity; (2) the potential impacts of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on our companies' cybersecurity and innovation efforts; (3) the broader effects of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on ecosystem cybersecurity for all industries; and (4) recommendations on how to best achieve the objectives of the Wassenaar Arrangement without compromising security objectives.

### **Cross-Border Data Flows and Cybersecurity**

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also 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 enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing 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 geographically-dispersed employees, 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.

Indeed, as well as facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for companies globally, helping to secure the systems and networks that manage production schedules and Human Resource (HR) data, as well as communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe. The Proposed Rule is part of a troubling global trend of erecting barriers to the free movement of global data, as also exemplified in the recent European court of Justice opinion effectively invalidating the Safe Harbor agreement.

Perhaps even more disturbing, the Proposed Rule, and the trend of impeding data flows generally, is contrary to the thrust of current U.S., and indeed global, cybersecurity policy.

To illustrate, as you know, late last year, Congress passed a bipartisan cybersecurity threat information sharing bill, the Cybersecurity Act of 2015.<sup>2</sup> The bill acknowledges that voluntary sharing of information

---

<sup>2</sup> Consolidated Appropriations Act, 2016, H.R. 2029, 114<sup>th</sup> Cong., Division N (2015).



regarding cyber threats, with appropriate privacy safeguards, is an integral component of improving our cybersecurity ecosystem, as it helps all stakeholders better protect and defend cyberspace. More specifically, Section 103 requires the heads of various federal security agencies to jointly develop procedures to ensure the Federal Government maintains “a real-time sharing capability.” Section 105 directs the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government receives and shares information about cyber threats, including via an automated real-time process, and Section 203 requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. President Obama signed the law, which aligns with the Administration’s consistent recognition of the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. For instance, also last year, President Obama issued Executive Order 13691,<sup>3</sup> which, among other things, states, “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.”

All of these policy efforts are intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity, and all of these initiatives contemplate the sharing of cybersecurity threat information as inclusive of information related to vulnerabilities. Given that the overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity, we are concerned that the Proposed Rule and the 2013 additions to the Wassenaar Arrangement could undermine this key principle and severely complicate the ability of companies in all sectors and government entities to share information in real-time to protect and enhance their security.

The onerous licensing scheme contemplated by the 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 recently advanced by U.S. government policymakers.

### **Potential Impacts of the Proposed Rule on Tech Sector Innovation and Cybersecurity Efforts**

The Proposed Rule would significantly damage cybersecurity technology innovation efforts by burdening companies with the onerous and time consuming process of applying for large volumes of unnecessary licenses. The damage could potentially impact a wide range of cybersecurity products and technologies in development, such as innovative defensive cybersecurity products, in addition to potentially restricting research into cyber vulnerabilities and exploits connected to valuable internal business activities, such as research and testing to determine vulnerabilities in our companies’ systems, products and technologies. Both of these sets of activities are intended to strengthen the cyber defenses of our companies and customers worldwide. 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 tools, and

---

<sup>3</sup> Exec. Order No. 13,691, 80 Fed. Reg. 9347 (February 20, 2015), available at <https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing>.



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.

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 actually exists, and 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 or 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 both individual companies to prepare license applications as well as for BIS to review and rule on them. It would also be extraordinarily time consuming. Months could pass between the time 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 Rule would be harmful to 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.

While concerning for any company doing business globally, the problems would disproportionately impact many companies in the tech sector, particularly companies developing software deployed across industry networks and the cloud, and security companies working to innovate solutions to help protect all stakeholders’ networks and systems.

Also troubling for these companies is language in the Proposed Rule empowering BIS to make the granting of licenses contingent upon companies’ disclosing their source code. The Proposed Rule states, “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.” We strongly urge BIS to reconsider any requirement that applicants 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.



## Broader Impacts of the Proposed Rule on Cybersecurity across Industry

Concerns regarding the Proposed Rule do not only impact the technology sector – they will negatively impact the ability of all companies to defend themselves from cybersecurity threats. All sectors, especially critical infrastructure, need effective cybersecurity, including the ability to share information quickly within sectors, among other sectors and with the Federal government, to discover and close vulnerabilities before they are widely known.

To be able to detect and remediate vulnerabilities – whether in products or systems – companies must retain the ability to identify and test those vulnerabilities. Even products that are not “specially designed” to perform the single intrusion function may be captured under the breadth of the Proposed Rule.

Most fundamentally, the Proposed Rule would do more to damage, rather than improve, the cybersecurity of U.S. companies, by restricting access to protective security measures required by networks all around the world. Imposing significant constraints on the ability of multinational corporations across multiple sectors to take cyber self-defense actions seems to belie common sense. For instance, companies’ vulnerability assessment teams use “intrusion software” to identify and track vulnerabilities in network devices and applications. The ability of companies to perform this activity across global boundaries, by sharing vulnerability information amongst their own-geographically dispersed or multi-national employees, should not be impeded.

Collaboration is most urgently needed during ongoing attacks. As stated above, the entire point of passing information sharing legislation was to facilitate the sharing of cybersecurity threat information, including information regarding security vulnerabilities, in as close to “real time” as possible so as to more quickly remediate them and minimize potential damage to companies’ networks. Potentially high-risk vulnerabilities are most valuable to hackers, and so are the exact type of cyber weaknesses that companies want to find during their internal penetration testing. Injecting a licensing scheme, with onerous requirements precluding intra-company transfers of critical cybersecurity threat information that would prevent companies from taking necessary defensive actions across their worldwide networks, seems to make little sense.

This problem is exacerbated by the Proposed Rule’s “policy of presumptive denial” for zero-day and rootkit capabilities, e.g., “product or system” or “delivery tool.”<sup>4</sup> 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 vulnerabilities, or zero-days, is the very same information that enables bad actors to exploit weaknesses in companies’ computer systems. If there is no technical difference defined in the Proposed Rule between the cybersecurity activities performed by our companies and the criminal activities performed by hackers, our companies will be significantly hampered by the imposed controls.

---

<sup>4</sup> Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28855 (proposed May 20, 2015), available at <https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>.



For the same reasons, the proposed export control regime could also impose severe limitations on information sharing beyond the walls of companies themselves, impacting established cybersecurity information sharing best practices more generally, including sharing within public-private partnerships (e.g., sector-coordinating councils and information-sharing and analysis organizations), and sharing linked to government contracts and protected programs. For example, 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.

Additionally, the portions of the Proposed Rule restricting surveillance items might also impact established best cybersecurity practices of companies. For instance, many companies utilize some type of packet analyzer (i.e. packet sniffer) to monitor and capture digital traffic passing over a network so that technicians can identify malicious code. The 2013 amendments to the Wassenaar Arrangement added the following to the list of dual-use goods: “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.”<sup>5</sup>

It is unclear how the inclusion of the restriction regarding IP network communications might impact the ability of companies to deploy their monitoring equipment and software in multiple locations on their networks to fight bad actors. Imposing licensing requirements that could impact such smart and basic cybersecurity practices seems both unfeasible and detrimental to enterprise security.

## Recommendations

The Proposed Rule raises a host of complex and interrelated technical policy issues involving usually disparate topics including cybersecurity, export control law, and human rights, and impacts government and industry interests alike. Given the diversity of impacted and knowledgeable stakeholders in these divergent areas, public-private collaboration in this issue area would greatly enhance the expertise of federal government representatives both at Wassenaar and in any future rulemakings.

Thus, at a minimum, we urge BIS to withhold publication of the Proposed Rule, and forgo further revisions with an eye toward implementation, and to instead engage the U.S. ICT industry, its inter-agency partners, and other stakeholders in detailed consultations regarding how best to achieve the 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 options and what further steps to take (likely in parallel) including, but not limited to:

- **Returning to Wassenaar to reopen the control, and in the interim, withholding the rule from publication.** Renegotiating the agreement is certainly a better option than simply not implementing the rule, which seems neither a prudent nor practical option. However, given that there appears to be wide variation amongst Wassenaar signatories in the implementation

---

<sup>5</sup> Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015), available at <https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>.



of the particular provisions impacting cybersecurity, clarifying the Wassenaar Agreement language itself seems the surest means of ensuring consistent implementation in a global cybersecurity environment.

- **Establishing a working group of technical experts from government and industry to systematically address both the technical and policy aspects of the cybersecurity, human rights and export controls considerations at issue.** As stated above, the Proposed Rule implicates competing equities and impacts multiple stakeholders. With this in mind, we call for the formation of an experts group to represent these competing interests and fully analyze the multiple facets of implementation of the 2013 Wassenaar Arrangement Plenary Agreement. We believe the experts group should have a broad charter and could examine any number of topics, including:
  - *Options for targeted implementation.* If reopening the control at Wassenaar proves unsuccessful and the U.S. has no choice but to implement the Proposed Rule, it is essential to work with security experts from government agencies and industry to devise an appropriate, targeted solution in consideration of all the dimensions of this important issue, so as to minimize the broader impacts. In particular, we advise examining how to limit the scope and coverage of the Proposed Rule via a narrower definition to avoid disrupting day-to-day business and security operations of global companies.
  - *Applicability of Pre-Existing Rules.* The experts group might explore whether any pre-existing rules might be applicable, or able to be modified, to address some of the legitimate human rights concerns underlying the rule.
  - *Targeting Bad Actors.* Exploring whether there is a way to target bad actors, as opposed to the current approach, which targets the technology. The experts group could focus on the variance between “defensive” and “offensive” cybersecurity measures, in an effort to 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 an information system. Enabling BIS to set appropriate export controls based on malicious end use which do not inadvertently subject companies, researchers and others to burdensome and onerous internal licensing requirements in order to conduct day-to-day business would be a win.

## Conclusion

Members of the subcommittees, ITI and our member companies are pleased you are examining how the Wassenaar Arrangement will affect the cybersecurity of our nation and private industry. The ICT sector is innovative and dynamic, continuously evolving as new products are developed and existing technologies are improved. However, the threats to our security also constantly change. Criminals and other bad actors modify and adapt their techniques almost as quickly as the industry is constantly innovating to address those threats. However, for our security efforts, and those of the federal government, to be effective, any cybersecurity regime implemented by government bodies must be flexible to allow government and private industry systems to leverage new technologies and business models, address constantly changing threat dynamics and manage new risks and vulnerabilities.



In addition, there are potentially broader international ramifications of pursuing policy approaches such as those embodied by the Proposed Rule. Whatever the rationale, the broad scope of the Proposed Rule could be viewed 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. Doing so would not only impose tremendous costs on some of the United States’ leading innovators and job-creators, but 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 stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to achieve the objectives underlying the Wassenaar Arrangement while also collectively improving cybersecurity innovation, risk management, and resilience.

Thank you.

**Committee on Oversight and Government Reform**  
**Witness Disclosure Requirement – “Truth in Testimony”**  
**Required by House Rule XI, Clause 2(g)(5)**

Name: **Dean C. Garfield**

---

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

**Personal: U.S. State Department, U.S. Speaker & Specialist Grant - \$4258**

---

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

**Information Technology Industry Council, President & Chief Executive Officer**

---

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

**None**

---

*I certify that the above information is true and correct.*

Signature:



Date: **1/8/2016**

---



## Dean C. Garfield President and CEO

Dean Garfield is the President and CEO of ITI. Since taking on this role in 2009, Dean has built ITI into the global voice of the tech sector and membership has nearly doubled. He leads a team of professionals who, combined, bring nearly three centuries of advocacy experience to bear on the most complex policy challenges facing the world's leading and most innovative technology companies.

Dean has worked to foster a policy environment that embraces cutting-edge research, game-changing technologies, and national economic champions as central to the foundation for sustained job creation and growth. The results: the tech sector has continued to grow despite global economic challenges. Companies are expanding -- putting more people to work, creating breakthrough products and services, and expanding into new markets with enormous opportunity. Under Dean's leadership, ITI has defined the tech agenda for global policymakers, expanded its membership and influence, and launched a foundation that serves as the preeminent thought leader on innovation. ITI has deepened its expertise on core issues -- from trade and new market development to taxes, from cloud computing to core standards. During Garfield's tenure, ITI's advocacy experts have helped to achieve critical legislative victories in the U.S. and internationally, knocking down barriers to innovation, strengthening America's economic competitiveness, and advancing sustainable technologies that will be at the heart of 21st century innovation.

Prior to joining ITI, Dean served as Executive Vice President and Chief Strategic Officer for the Motion Picture Association of America (MPAA). While there, he developed the association's global strategies, securing accomplishment of key operational objectives, forged industry alliances on behalf of the MPAA, and led the MPAA's Research and Technology Departments. Dean also represented the MPAA before legislative bodies and at key conferences around the world, including the European Commission and Oxford University.

Dean also served as Vice President of Legal Affairs at the Recording Industry Association of America (RIAA). He helped to develop the organization's comprehensive intellectual property policy and litigation strategies and managed several of the United States' most important intellectual property cases, including the Grokster/Kazaa case, from its filing to its resolution at the Supreme Court.

He received a joint degree from New York University School of Law and the Woodrow Wilson School of Public Administration and International Affairs at Princeton University. He was a Ford-Rockefeller as well as a Root-Tilden-Snow scholar.

In 2015, Dean was named Top Lobbyist by The Hill for his leadership of ITI and his work with companies and stakeholders to make tech a more diverse and inclusive industry. Dean was honored with the first REACH Breaking Barriers Award in May 2010, recognizing him for his deep commitment to leading the world's most dynamic industry in its efforts to support and inspire young people to develop the important science, technology, engineering and math (STEM) skills they must have to become tomorrow's scientific problem solvers. Dean serves on the boards of College for Every Student, the SEED School of Washington, D.C. and serves as the Board President of Aiden Montessori School. He has been featured in several national publications, on National Public Radio, CNBC, and Bloomberg TV News, representing the tech industry on the issues that matter most to the sector.

**Written Testimony of Cristin Flynn Goodwin  
Assistant General Counsel for Cybersecurity at Microsoft Corporation**

**Oversight and Government Reform Subcommittee on Information Technology  
Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security  
Technologies**

**Joint Subcommittee Hearing on Wassenaar: Cybersecurity & Export Control  
January 12, 2016**

**Introduction**

Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and members of the Subcommittees, my name is Cristin Flynn Goodwin, and I am Assistant General Counsel for Cybersecurity at Microsoft Corporation. I advise a wide-range of teams inside Microsoft on cybersecurity legal issues globally and I oversee Microsoft's Government Security Program, where we work with governments around the world on security.

Microsoft is a global company operating in over 120 countries, with services and products that consumers, enterprises, and governments use on a daily basis. Eighty percent of the Fortune 500 and millions of consumers rely on our cloud services.<sup>1</sup> This growth and scale in our cloud business helps us appreciate the complexity of meeting security challenges and protecting customers around the world. It is Microsoft's commitment to security that brings me here today to discuss our assessment of the challenges in implementing the Wassenaar Arrangement's controls agreed to at the December 2013 Plenary on intrusion software and related items.<sup>2</sup>

As the Subcommittees know well from the recent success on the Cybersecurity Act of 2015, legislating cybersecurity requires a deep understanding of the problem space, broad input from experts and the private sector to ensure thoughtful technical impact and applicability, support from major stakeholders in the Executive Branch, and the open and well-known legislative process to move the issue forward. In the case of the intrusion software definition coming out of the Wassenaar Arrangement, and its proposed implementation from the Department of Commerce, this issue does not reflect the same sort of consensus.

The proposed definition, if left unchanged and implemented, applies "almost universally to the building blocks of security research" and will have a "chilling effects on the development of anti-surveillance

---

<sup>1</sup> "Satya Nadella and Scott Guthrie: Microsoft Cloud Briefing," Microsoft News Center, October 20, 2014, available at: <http://news.microsoft.com/speeches/satya-nadella-and-scott-guthrie-microsoft-cloud-briefing/>.

<sup>2</sup> The Wassenaar Arrangement is a 41-nation regime designed to advance "regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies." Its members include a majority of European nations, as well as Canada, Russia, Japan, and Australia. The Agreement aims to prevent destabilizing accumulations of certain capabilities and to prevent the acquisition of these items by terrorists.<sup>2</sup> Wassenaar is a consensus-based organization; once consensus is reached, the Member States implement the agreements domestically in accordance with local legislation. Quote and information available at [www.wassenaar.org](http://www.wassenaar.org).

measures and on the discovery of existing vulnerabilities.”<sup>3</sup> We have the opportunity to re-set the international approach and its domestic implementation, and ensure that security responders and technology innovators around the world can respond to threats and vulnerabilities in real-time, as they do every day. At a time when we are all looking to empower security defenders and provide them with the tools and capabilities they need, we cannot take a significant step backwards.

Microsoft strongly encourages Congress and the US Government to re-engage Wassenaar Arrangement member states, undo the overly broad, overly complicated export control requirements, and suspend any related rulemaking efforts until a new agreement can be reached.<sup>4</sup> As a committed participant in the public private partnership in the United States, we are eager to engage on cybersecurity regulation and to provide any technical expertise and perspective needed going forward.

We commend both subcommittees for examining the use of export control regimes to regulate cybersecurity, and we welcome the opportunity to contribute to this important dialogue.

My testimony will focus on four areas:

1. The Wassenaar definition of intrusion software and the problems that arise from the overbroad definition and controls;
2. The impact of the proposed regulatory approach on innovation and security response;
3. The importance of the public private partnership in cybersecurity regulation; and
4. The role of governments in establishing cybersecurity norms that curtail the uses of surveillance technologies.

## **1. Why Words Matter: Defining the Problem and “Intrusion Software”**

### *a. Defining the Problem*

Microsoft is a staunch supporter of the principle that technology should not be used to violate human rights, or to harm or impede those that seek to advance the cause of human rights. In that vein, the original intent of the Wassenaar Arrangement drafters is admirable and important. Unfortunately, due to the overbroad definition of intrusion software, the broad scope of items subject to control, and the burdensome licensing requirements proposed in the United States, this Proposed Rule would create a set of regulations that constrain security and innovation and may diminish the capabilities of enterprises and people to secure themselves against increasingly persistent and sophisticated cyber threats.

Although many Wassenaar proceedings are confidential, Microsoft understands that the original intent behind these controls was to restrict the export of sophisticated surveillance systems to authoritarian governments. Such systems, like those developed and sold by companies like Gamma Group (owner of FinFisher) and Hacking Team are reportedly used to spy on or otherwise repress political dissidents and

---

<sup>3</sup> “Why Wassenaar’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk – And How To Fix It”, Sergey Bratus, et al., October 9, 2014, available at: <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.

<sup>4</sup> For additional detail on the challenges with the Proposed Rule, please consult Microsoft’s “Comments on Wassenaar Arrangement Plenary 2013: Intrusion and Surveillance Items” available at: <http://mscorp.blob.core.windows.net/mscorpmedia/2015/07/Microsoft-Intrusion-Software-Submission-BIS-2015-2011-RIN-0694-AG49..pdf>.

other citizens.<sup>5</sup> These sophisticated turnkey systems are claimed to permit the targeting and monitoring of an individual's phone calls, emails, and other communications.

Limiting the sale of sophisticated surveillance technologies to governments or other entities that could abuse the technology and violate laws or rights of others is a very real and very important challenge that needs to be addressed. Appropriately tailored export control regulations may be one part of an overall approach to controlling transfers of these technologies. However, in order to address concerns about abuses of surveillance software, or other similar topics in the future, it is important that the involved governments clearly articulate the challenge and engage technical experts from the private sector well before future Wassenaar votes take place. Given the broad dissent and need for clarity on the problem scope, applying principles from the cybersecurity norms discussion and driving for broader nation state and industry consensus prior to international agreement and regulation is a better approach. Due to the fact that the intrusion software issue has already gone through Wassenaar voting, it may be more realistic to encourage Wassenaar members to apply the principles of the cybersecurity norms debate to its work and reset this discussion from the beginning.

*b. Defining Controls Related to Intrusion Software*

The Wassenaar members in 2013 used a very challenging approach to try to define what it sought to control. First, as has been commented on by many stakeholders, the Wassenaar Arrangement agreed to a very broad definition of "intrusion software":

*Software specially designed or modified [i] to avoid detection by monitoring tools, or [ii] to defeat protective countermeasures, of a computer or network-capable device [including mobile devices and smart meters], and [iii] 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.*

To those who are not technical information technology (IT) experts that definition might appear quite narrow. However, it "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

---

<sup>5</sup> See, e.g., Bill Marczak, Written Evidence to the UK Parliament, *Export of British-Made Spyware Targeting Bahraini Activists*, November 19, 2012, available at: <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmfaaff/88/88vw43.htm>; see also Response of the UK Secretary of State for Business Innovation and Skills, *Export Controls for Surveillance Equipment - Proposed JR*, August 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](https://web.archive.org/web/20140816043658/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_08_08_response_from_tsol.pdf).

reliability and monitoring, and operating systems.”<sup>6</sup> Then, in an added layer of complexity, the Wassenaar controls and licensing obligations are applied to the following items *related* to such intrusion software (among other items):

- (a) Systems, equipment, components and software specially designed or modified for the generation, operation or delivery of, or communication with intrusion software; and
- (b) Technology (*i.e.*, technical data and technical assistance) for the development of intrusion software, or for the development, production or use of equipment or software specified in (a) above.

Because the Wassenaar Arrangement text is not self-executing, each member state then in turn implements the agreed-upon controls domestically. The United States implementation was proposed by the Department of Commerce (Commerce) Bureau of Industry and Security (BIS), in a Federal Register notice in May 2015 (“Proposed Rule”) that took some in the security community by surprise.<sup>7</sup>

Security teams around the world looked at the overbroad definition, exacerbated by the BIS proposal on implementation, and the reaction from the security community was quite vocal, questioning how it would be possible to continue developing new products and services, or to fight attacks and threats, if the proposed regime became the law in the United States. Microsoft engineers expressed concern that, if implemented, triaging vulnerabilities with security researchers in the Microsoft Security Response Center<sup>8</sup>, assessing malware in the Microsoft Malware Protection Center<sup>9</sup> or developing tools with internal teams could become a burdensome and time-consuming exercise of government filings, documentations, and forms, and not innovation.

This reality is already affecting the security community. One security conference was cancelled in Japan, citing “the complexity of obtaining real-time import/export licenses in countries that participate in the Wassenaar Arrangement. . . .”<sup>10</sup> The prospect of untangling a web of export filings for a cadre of

---

<sup>6</sup> “Why Wassenaar’s Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk – And How To Fix It”, Sergey Bratus, et al., October 9, 2014, available at: <http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf>.

<sup>7</sup> “Head Scratching Begins on Proposed Wassenaar Export Control Rules,” Michael Mimoso, Threat Post, May 21, 2015, available at: <https://threatpost.com/head-scratching-begins-on-proposed-wassenaar-export-control-rules/112959/>. See also, “Experts Concerned About Effects of Proposed Wassenaar Cybersecurity Rules,” Eduard Kovacs, Security Week, May 26, 2015, available at: <http://www.securityweek.com/experts-concerned-about-effects-proposed-wassenaar-cybersecurity-rules>.

<sup>8</sup> More information about the Microsoft Security Response Center available at: <https://technet.microsoft.com/en-us/library/dn440717.aspx>.

<sup>9</sup> More information about the Microsoft Malware Protection Center available at: <http://www.microsoft.com/security/portal/mmpc/default.aspx>.

<sup>10</sup> “Pwn2Own Tokyo hacking contest trashed, export rules blamed” Richard Chirgwin, The Register, September 3, 2015, available at: [http://www.theregister.co.uk/2015/09/03/pwn2own\\_tokyo\\_trashed\\_wassenaar\\_blamed](http://www.theregister.co.uk/2015/09/03/pwn2own_tokyo_trashed_wassenaar_blamed) (quoting official from the event’s sponsor).

international security researchers working in real-time to create security solutions to challenging problems simply stifled the research altogether. Even before implementation, the overbroad definition and scope of the controls are already having an impact on the security community's ability to collaborate and respond.

## **2. Impact of the Current Approach on Innovation and Cybersecurity**

### *a. How Microsoft is Impacted by the Current Wassenaar Approach*

Microsoft has devoted significant resources and personnel to extensive, critical, and time-sensitive research and development and other defensive security activities to protect our software, our services, and our networks against cyber and other security vulnerabilities. This work is essential not only to protect Microsoft's own networks and services, but more broadly to protect the networks and data of Microsoft's customers and users, including US Government users, such as the Congress of the United States. These activities, which are vital to protecting our nation's IT infrastructure, would be severely impeded by the Proposed Rule if implemented as drafted.

Given the global nature of product development and *defensive* security activities and the involvement of nationals from dozens of countries — including employees of Microsoft and its large number of third party security partners — Microsoft estimates that current activities would require the issuance by BIS of hundreds or thousands of export licenses. Millions of Microsoft customers, including the US Government, would likely face increased software and other security vulnerabilities that could be exploited by state and non-state actors, and our customers, as well as the security community, would feel the impact of slower incident response, and delayed product updates and services as security is put on hold due to licensing obligations.

Internally, Microsoft has a diverse community of teams involved in security. Some of these teams are well known, like the Microsoft Security Response Center, the Microsoft Malware Protection Center, or the Digital Crimes Unit<sup>11</sup>. Others are more internally focused, and concentrate on product development (such as Windows or Office and our cloud services). Microsoft Consulting Services also supports client security needs around the world, including the US Government and government contractors. Each of these teams includes significant numbers of non-US citizens.

Here is an example of a type of event that happens over 1,000 times a year at Microsoft. The Microsoft Security Response Center (MSRC) receives an unsubstantiated tip from a researcher in Switzerland, which claims to contain a proof of concept of a vulnerability, some reproduction code, and a tool that the person used to get the vulnerability to reproduce. The MSRC employee, a US national, needs to discuss the technical details of the proof of concept in order to validate the vulnerability, but to reach back to the researcher in Switzerland, he would likely need a license (or at least spend time determining whether a license is needed). Instead, he reaches out to another employee on his team to help. She is a citizen of Poland working in the UK. If not already authorized, our US national needs to contact Microsoft's Global Trade team which will help the employee prepare a filing to obtain a license to do that validation. The license application will take 6 – 10 hours to prepare, and then approximately 30 days to be approved. Once approved, and the technical exchanges occur, the MSRC validator writes some code that helps her test the vulnerability and test a potential idea for mitigation, along with an

---

<sup>11</sup> More information on Microsoft's Digital Crimes Unit available at: <http://news.microsoft.com/presskits/dcu/>.

accompanying technical explanation. However, before these materials can be shared with the development organization, including developers of many nationalities, additional licenses may be needed to share the information with the developers, depending on their nationalities. This is simply an unworkable process just to start an investigation for certain vulnerabilities.

*b. Specific Examples of Impact Arising out of the Intrusion Software Definition*

The private sector has voiced significant concerns over the overbroad intrusion software definition as well as the related technology and software controls. Microsoft has identified nine different areas of major impact in the security space should these controls remain in place, and the implementation adopted. Each of these areas is detailed below, and ranges from present and immediate concerns (as in the ability to deploy penetration testing tools) to more forward-looking concerns (such as machine to machine sharing creating an export or re-export licensing obligation). In all of these areas, Microsoft’s security teams are not simply passive recipients of information or tools; to be effective and timely, the teams must be engaged in active creation, response and sharing of software and technology that is likely to be controlled under the Proposed Rule.

Issue	Description	Used For
<b>Penetration Testing</b>	Software created or used to evaluate and improve the security of services and software that Microsoft develops and operates. Includes proprietary software and open-source software that Microsoft has specially designed or modified for particular purposes.	Used to monitor internal systems, ensure compliance with security policies, and help protect systems. Microsoft also reverse engineers pen testing tools used by bad actors in order to protect customers.
<b>Malware Research</b>	Malware, exploit code, and reported vulnerabilities, including malware that meets the definition of intrusion software.	Microsoft performs extensive analysis on malware, including reverse engineering the code to identify how it was put together. Microsoft also creates <i>new</i> code, including new intrusion software, to illustrate the risks of the particular malware or malware family
<b>Vulnerability Testing</b>	Similar to penetration testing, Microsoft uses both proprietary tools and open source tools that are specially designed or modified in response to specific intrusion software-related attacks.	Mitigating impacts of vulnerabilities, identifying new vulnerabilities, and enabling software engineers to reproduce and test software patches, updates, and upgrades.
<b>Security Tools</b>	This is a broader class of tools used in security, including debuggers, file	Identifying vulnerabilities, modifying software to enhance operability or decreasing security risks

	fuzzers, and other automation used to support security.	
<b>Application Compatibility, Interoperability and Work-Arounds</b>	Microsoft develops and deploys “shims” which are technology “work-arounds” to aid in the compatibility of software programs with its operating systems.	Shims or work-arounds modify the intended function or path of a file in order to enable compatibility with other devices or interoperability with other software.
<b>Information Sharing</b>	Receiving and sharing thousands of threat reports, vulnerability issues, and other security related issues on Microsoft products and services and third party products and services in the Microsoft ecosystem. Collaborating on planned and ad hoc issues that arise on security.	Incident response, mitigating vulnerabilities, investigating new issues, sharing information to help raise security awareness amongst others, and generally protecting the computing ecosystem.
<b>Supporting Customers</b>	Microsoft Consulting Services provides technical and other services on-site with customers around the world leveraging Microsoft tools and technologies.	Used to investigate breach responses, conduct penetration tests, review software and security issues, and create recommendations on improving security.
<b>Engaging the Security Community</b>	Working directly with security researchers, third-party companies, hosting competitions, participating in conferences, and engaging on difficult security issues to improve product and services security.	Includes sharing information, technology, tools, ideas, and collaboration; can include hosting “bug bashes” or awarding prizes, <sup>12</sup> paying for “bug bounties,” publishing research, <sup>13</sup> attending conferences, and creating new tools, technologies, and tactics to improve security.
<b>Automated Exports and Re-Exports</b>	Automation is the future state of security and is continuing to change the security landscape. Machine to machine information sharing allows automation and machine learning to make adjustments without human interaction, although the	Microsoft engages in a growing use of automated software programs and custom developed tools, which can include software that automatically exports and re-exports items; the Proposed Rule

<sup>12</sup> See, e.g., Microsoft’s Blue Hat Prize: <http://www.microsoft.com/security/bluehatprize/>.

<sup>13</sup> “UK Student’s Research a Wassenaar Casualty,” Michael Mimoso, threatpost.com, July 6, 2015, available at: <https://threatpost.com/uk-students-research-a-wassenaar-casualty/113625/> (highlighting a restricted portion of the student’s dissertation on expanding bypasses for Microsoft’s Enhanced Mitigation Experience Toolkit).

	information can move between US and non-US servers.	does not yet contemplate machine to machine exports and re-exports.
--	---	---

*c. The Impact of the Licensing Burden on Industry and BIS*

The Wassenaar Arrangement specifies *what* is to be controlled, but does not identify specific levels or methods of control that each member state should apply. The US licensing requirements that would be imposed under the Proposed Rule compound the serious problems created by the overbroad Wassenaar definition of what is controlled. While other Wassenaar members appear to apply a permissive licensing regime, the United States proposes to require specific prior export licensing for virtually any export or re-export - including disclosures to foreign nationals in the United States - of any controlled item to any destination other than Canada.

Microsoft estimates that the Proposed Rule would require hundreds or thousands of licenses for the export, re-export, and/or deemed export of items. Microsoft has an experienced and well-developed export control compliance program; however, no compliance team could prepare this many license applications, to say nothing of managing compliance with the terms and conditions of issued licenses. The burden on development and security teams to assist in the creation and completion of and compliance with these licenses would clearly impact product and service creation, customer support, and security. Today, an average license submission with readily available contacts and information needed takes between 6 to 10 hours to prepare. For more complex licenses or issues that require more technical investigation, that range can increase significantly.

It is a reasonable presumption that BIS will lack the capacity to review and issue the volume of licenses for all of the companies, universities, individual researchers, and other organizations that will require such licensing. Today, we expect an average of 30 days to receive an approval on a license application, with more complex issues taking 90 days or longer. Waiting periods will likely increase as the volume of licenses increases exponentially.

Moreover, the involvement of foreign nationals (either employed by Microsoft or a third party) occurs in every facet of security today. Response occurs 24x7, using “follow the sun” capabilities, whereby security issues are transferred to teams in different time zones so that security work can progress around the clock. This real-time activity cannot be postponed for days, let alone weeks or months, while Microsoft prepares a license application and BIS processes it, including referral to the Defense Technology Security Administration. 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 re-exported, the identity of the foreign nationals or entities receiving it, and destinations with whom the items will be shared, generally will not be known in advance.

Finally, as part of some of the activities described above (to investigate or mitigate threats), in some instances Microsoft exports and re-exports items that have or support rootkit and/or zero-day exploit capabilities. According to the preamble to the Proposed Rule, a policy of presumptive denial would apply to license applications for such items, and therefore exports and re-exports that are a core aspect of critical security activities apparently would be prohibited from occurring, putting customers at risk.

*d. Impact on Congressional Priorities*

The US Congress recently passed information sharing legislation that would facilitate the sharing of cyber threat information within the private sector, as well as between the private sector and the government. The proposed regulation has interesting ramifications for the Cybersecurity Act of 2015 as well. As the Subcommittees are well aware, widespread sharing of information about threats, vulnerabilities, and adversary capabilities and techniques is critical to ensuring security and privacy. Those exchanges happen internally within companies, and externally, with vendors and partners, with the security research community, and with the government. In many cases, those exchanges are impromptu and ad hoc and stem from emerging security issues or discoveries, such as a script that a security researcher may write to help assess a new piece of malware. Therefore, whether internal or external, the proposed regulation could require a license for exchanges that the legislation had intended to encourage and accelerate.

What's more, as emphasized by the legislation, a significant trend in information sharing is automation and sharing in real-time, at machine speed. That type of sharing could similarly be impacted when the data is shared across national borders or shared domestically with persons from outside the United States. Administration policy as stated in Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, promotes information sharing, as do Congress's recent cybersecurity achievements, but the proposed intrusion software definition and its implementation could have a chilling effect on reaching Congress's goals.

*e. Global Challenges Arising out of Wassenaar Implementation*

One of the challenges Microsoft faces as a company with software developers in a number of countries is that Microsoft needs to be able to comply with a range of export control regimes. Many governments have been watching the rollout of the US approach with interest. The United Kingdom's approach also requires licensing<sup>14</sup> and is problematic in that it, too, struggles with the same overbreadth of the underlying definition of intrusion software. While the UK's license exceptions are broader, it remains our view that a large number of licenses may be required to comply with the UK regime. We are continuing to assess the guidance. Other nations have not yet published specific guidance on how to comply with the intrusion software obligations. Some governments have expressed concern about the recent Wassenaar action, including India, which convened senior government officials to review the impact of the potential regulation for Indian companies.<sup>15</sup>

The United States should take a leadership role on cybersecurity issues in the export control space and work with the international community to develop a more narrowly-tailored and outcome-focused approach, rather than leave the current approach in place.

### **3. The Public Private Partnership and Cybersecurity Regulation**

---

<sup>14</sup> "Notice to Exporters 2015/24: ECO issues guidance on intrusion software controls," Department for Business, Innovation & Skills, August 10, 2015, available at: <http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/>.

<sup>15</sup> "Indian Officials see cyber threats from Wassenaar Arrangement", The Economic Times, June 19, 2014, available at: [http://articles.economictimes.indiatimes.com/2014-06-19/news/50711034\\_1\\_cyber-threats-inter-ministerial-panel-software-products](http://articles.economictimes.indiatimes.com/2014-06-19/news/50711034_1_cyber-threats-inter-ministerial-panel-software-products).

The “Public Private Partnership” is one of the foundational principles of cybersecurity in the United States. It has been cited in countless speeches by Government and private sector representatives at all levels, and is recognized as essential to creating smart regulatory and technical responses to cybersecurity challenges. The public private partnership is also important to ensure that information is shared, threats assessed, and critical issues mitigated before attacks or consequences can disrupt key services.

*a. Wassenaar Arrangement Proposals and the Public Private Partnership in the US*

The negotiation of Wassenaar proposals typically begins with a proposal from a member state. In the United States, there are a number of advisory committees hosted by the Department of Commerce that are used to help formulate a private sector view on the proposals before US Government representatives go to Wassenaar meetings to negotiate with the other member states.

In this case, the intrusion software proposal appears to have originated with the United Kingdom, which was seeking to control sophisticated surveillance software such as those sold by the UK company Gamma International (maker of FinFisher), and the Italian company Hacking Team, as products from those companies had been identified in attacks against “political dissidents and other activists.”<sup>16</sup> In assessing the outcome of the Wassenaar process, however, one leading technology association noted, “Unfortunately, the negotiators of these provisions lacked technical expertise and defined ‘intrusion software’ far too broadly.”<sup>17</sup>

Once the Proposed Rule reached the security community in May 2015, it was immediately clear to industry that what was agreed upon in December 2013 was unworkable.

*b. The Public Private Partnership, Cybersecurity and Export Control*

Fortunately, the US has a good track record overall of Congress, the private sector and the Executive Branch working together in many areas to solve difficult problems, including those involving both cybersecurity and export control. We submit that the scope of controls related to intrusion software needs to be reconsidered, and there needs to be a plan for ongoing private sector consultation as the revision of these controls is pursued. In addition, we continue to hear that issues beyond intrusion software are looming in the not-so-distant future for Wassenaar consideration. Working with our colleagues in industry, the Congress and the Executive Branch, we should be able to have a robust process in place that can address security interests without impacting security or impeding innovation.

#### **4. Cybersecurity and Changing Global Norms**

---

<sup>16</sup> “The Wassenaar Arrangement: Overview,” BSA, the Software Alliance, (BSA Overview) available at: <http://www.bsa.org/~media/Files/Policy/IssueBriefs/12072015Wassenaar.pdf>; see also, “Hacking Team sold Spyware to 21 Countries; Targeting Journalists and Human Rights Activists,” Swati Khandelwal, The Hacker News, February 24, 2014, available at: <http://thehackernews.com/2014/02/hacking-team-sold-spyware-to-21.html>; see also “Ethopia: Hacking Team Lax on Evidence of Abuse – Human Rights Watch,” Ethiopian Team, August 15, 2015, available at: <http://ethiopianteam.net/ethiopia-hacking-team-lax-on-evidence-of-abuse-human-rights-watch/>.

<sup>17</sup> See BSA Overview at 12.

One of the issues that has been brought to the surface through both the intrusion software discussion and the disclosure of the emails of Hacking Team is that governments, including those who may seek to suppress dissent, are often the customers of the technologies at issue here.<sup>18</sup> What is also clear is that different governments, including various Wassenaar signatories, will use technology and tools in ways that the United States and other nations find unacceptable, and that while some states agree on the need for export control of surveillance software, others find its use acceptable.

This issue of the use of surveillance software may be appropriate for analysis along the lines of the cybersecurity norms debate. Microsoft has observed five important principles that should underlie international discussions of cybersecurity norms: harmonization, risk reduction, transparency, proportionality, and collaboration. “These principles are important to keep in mind when governments are discussing which issues of cybersecurity rise to the level of normative behavior, which require conventions among a large number of states, or smaller, bilateral or multilateral agreements, or which are simply adopted into domestic laws or public policies.”<sup>19</sup>

We believe that applying the principles of the cybersecurity norms debate to surveillance software and potentially other issues arising in export control of cybersecurity is that it helps ensure agreement and understanding among governments and the private sector.

Our goal – albeit ambitious – is to prevent the emergence of a world where cyber conflict undermines trust. The alternative is to realize too late, among the wreckage, that something should have been done long ago. Cybersecurity norms that limit potential conflict in cyberspace are likely to bring greater predictability, stability and security to the international community.<sup>20</sup>

## 5. Conclusion

Microsoft welcomes the Subcommittees’ interest in this matter and their oversight and guidance on how the public private partnership can continue to help advance the state of cybersecurity in the United States. We believe that this important issue is a bellwether for future cybersecurity activity, and it is important that the US demonstrates clear and principled leadership as we contemplate future regulation impacting cybersecurity.

---

<sup>18</sup> “Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim”, Alex Hern, The Guardian, July 6, 2015, available at: <http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim> (noting that “if genuine, Hacking Team’s clients are the governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE, many of whom have been criticized by international human rights organizations for their aggressive surveillance of citizens, activists, and journalists both domestically and overseas.”)

<sup>19</sup> “Five Principles for Shaping Cybersecurity Norms,” Microsoft, available at: [file:///C:/Users/cgoodwin/Downloads/Five Principles Norms%20\(1\).pdf](file:///C:/Users/cgoodwin/Downloads/Five%20Principles%20(1).pdf).

<sup>20</sup> “Proposed Cybersecurity Norms to Reduce Conflict in an Internet-dependent World,” Paul Nicholas, Cyber Trust Blog, December 3, 2014, available at: <http://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/>.

**Committee on Oversight and Government Reform**  
**Witness Disclosure Requirement – “Truth in Testimony”**  
**Required by House Rule XI, Clause 2(g)(5)**

Name: Cristin Flynn Goodwin

---

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

I have not received any federal grants, subgrants, contracts or subcontracts.

---

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

I am testifying on behalf of my employer, Microsoft Corporation, where I am Assistant General Counsel for Cybersecurity in Microsoft's Trustworthy Computing division. In this capacity I lead Microsoft's Government Security Program (GSP) providing security support to governments. I also provide legal counsel to Microsoft's businesses and teams on a wide range of cybersecurity issues.

---

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

Microsoft Corporation does business with almost every federal agency. To the best of my knowledge, Microsoft does not receive grants or subgrants from the federal government. Microsoft does have some direct consulting and product support contracts with the federal government. However, most of Microsoft's business with the federal government, in particular software and online services, is conducted through reseller channels where Microsoft serves as a subcontractor under agency-wide agreements, the GSA Schedule or similar contract vehicles.

---

*I certify that the above information is true and correct.*

Signature:

Date:



1/7/2016

---

Cristin Flynn Goodwin is the Assistant General Counsel for Cybersecurity in Microsoft's Trustworthy Computing division. Cristin leads Microsoft's Government Security Program (GSP) which provides governments with a structured, legal means to access source code and affirm there are no back doors in Microsoft products or services, as well as to share information about threats and vulnerabilities. She helped launch the GSP's Transparency Centers in June of 2014 to enable secure government access to source code in response to the Edward Snowden allegations. Since 2008, she has been Microsoft's lead counsel for all aspects of Microsoft's security incident response processes and security updates for over a billion customers around the world. Cristin also provides legal counsel for Microsoft's cyber security public policy worldwide, supporting her clients and legal and policy experts in Microsoft's subsidiaries worldwide.

Cristin joined Microsoft in 2006, where she initially served as policy counsel in Microsoft's Washington, DC office. Prior to joining Microsoft, Cristin worked for BellSouth, and served in an operational role on a wide range of policy and operational issues, including during hurricanes Katrina, Rita, and Wilma in 2005, as well as Charley, Frances, Ivan and Jeanne in 2004, in addition to other National Security Special Events.

Prior to joining BellSouth, Cristin was policy counsel at MCI, where she specialized in cyber security, backbone network security and infrastructure protection issues, and was actively engaged in MCI's response to 9/11, and the myriad of policy, technology and legal work that ensued with the Federal government in the years following 9/11. Cristin began her career as a trial lawyer in New York City.

Cristin currently lives in Redmond, Washington with her husband and two children.



Prepared Testimony and  
Statement for the Record of

**Cheri F. McGuire**  
**Vice President, Global Government Affairs & Cybersecurity Policy**  
**Symantec Corporation**

Hearing on:

**“Wassenaar: Cybersecurity & Export Control”**

Before the

House Committee on Homeland Security  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

and

House Committee on Oversight and Government Reform  
Subcommittee on Information Technology

January 12, 2016

2154 Rayburn House Office Building

Chairman Ratcliffe, Chairman Hurd, Ranking Members Kelly and Richmond, and distinguished members of the Committees, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. Currently I serve on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of the George Washington University Center for Cyber and Homeland Security, the Information Technology Industry Council, and the National Cyber Security Alliance. From 2010 to 2012 I served as the Chair of the U.S. IT Sector Coordinating Council – one of 16 critical infrastructure sectors identified by the President and the U.S. Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec protects much of the world's information, and is the largest security software company in the world, with 33 years of experience developing computer security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services (Symantec for enterprises and Norton for consumers and small businesses) protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording thousands of events per second, and more than 500 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts and our security technologies a unique view of the entire Internet threat landscape; which in turn we use to protect our customers' most sensitive data and systems around the world.

## **Introduction**

The hearing you are holding today is extremely timely. It shines a spotlight on a critical issue that threatens the cybersecurity of not only the U.S. technology industry, but also that of all U.S. critical infrastructure companies and organizations that operate or connect to networks overseas. The proposed U.S. cybersecurity export control rule under the Wassenaar Arrangement would severely damage our ability to innovate and develop new cybersecurity products, to conduct real time global research and share information on software vulnerabilities and exploits, and to test and secure global networks and new technology products.

These restrictions would devastate the U.S. cybersecurity industry itself and harm the security of nearly every U.S. multinational company. This rule is not an export control on a few specific tools. It is a stringent new regulation on the entire cybersecurity industry and its customers that would harm the economic and national security of the U.S. Ultimately, it would leave every American less protected against cybercriminals and cyber terrorists.

Industry and academia in the U.S. are at the forefront of designing, testing and developing some of the world's leading cybersecurity technologies. Companies like Symantec rely on unfettered research and communication to innovate and develop the next generation of security technologies. These new regulations would restrict this free-flow of information and impose major new export compliance burdens on all U.S. multinational industries. It would have three significant negative impacts on cybersecurity:

- First, cybersecurity research would be curtailed, as the rule hinders developers and researchers from testing products and networks and sharing technical information about new vulnerabilities and exploits across borders.
- Second, the availability of critical cybersecurity tools would be constrained, as the rule restricts the export of cybersecurity technologies, even to subsidiaries of U.S. companies overseas.
- Third, cybersecurity collaboration and information sharing would be harmed, as the rule deems information to be “exported” once it is shared with non-U.S. persons, even if they physically work for a company here in the U.S.

The significant time and effort that both the government and the private sector have spent jointly searching for a way to redraft the rules has not borne fruit, but not because of a lack of good faith on both sides. The effort has failed because the proposed rule contains unresolvable ambiguities and fundamental flaws – defects that are rooted in the faulty original 2013 Wassenaar cybersecurity agreement. For this reason, the U.S. redrafting effort should be suspended. The U.S. government should take a leadership role and return to Wassenaar in the upcoming plenary session with a proposal to renegotiate the original 2013 cybersecurity agreement.

In my testimony today, I will discuss:

- An overview of the Wassenaar Arrangement and the “cybersecurity rule”;
- Consequences for cybersecurity tools, testing, research and information sharing;
- Other critical infrastructure sectors affected by the rule;
- Economic impacts of the rule for industry and the government;
- How other Wassenaar nations are implementing the rule; and
- Why the U.S. proposed rule is unworkable, and solutions outside of Wassenaar.

## **I. Overview of the Wassenaar Arrangement and the “Cybersecurity Rule”**

The Wassenaar Arrangement is a multilateral export control agreement with 41 nations as signatories that was designed to cover conventional arms and dual-use goods and technologies and prevent proliferation of sensitive components. It did not originally envision, nor was it designed for, widely available cybersecurity software technologies. There is a process for adding new controls, and under the 2013 agreement, the United Kingdom offered a proposal that “intrusion” and “surveillance” software be added to the list of export-controlled technologies. This grew out of well-intended concerns over the availability of “intrusion software” to abusive regimes and the need to protect dissidents. As the control was being developed, we are not aware of any consultations with the U.S. cybersecurity industry about its real world implications, given that the underlying software functionality of intrusion software is the same or similar to other widely used security technologies.

Though the Wassenaar Arrangement is non-binding, it has long been the policy of the U.S. to fully implement agreements under it and to update its own export control regime accordingly. As part of the U.S. implementation of this new control, in May 2015 the Department of Commerce (DoC) published for comment in the Federal Register a proposed amendment to the U.S. export regulations that would cover cybersecurity products categorized as “intrusion and surveillance items.” Due to the overly broad definitions in the Wassenaar control and the subsequent U.S. rule, industry and academia submitted an unprecedented volume of approximately 300 formal comments, nearly all of them strongly objecting to the new regulations.

Symantec, like many others, demonstrated that the rules were written far too broadly and hindered legitimate, widely used and beneficial cybersecurity technologies and practices, including penetration testing software, white-hat research, and cyber threat information sharing. Since the initial comment

period, the DoC has proactively engaged in an impressive amount of outreach to solicit advice and input on how they could implement the rule in a way that would not severely damage U.S. economic and national security.

However, the underlying language negotiated at the 2013 Wassenaar Arrangement Plenary was so deeply flawed that, despite months of consultation, we still cannot envision language that would mitigate the numerous detrimental effects. The core problem is that the needed changes do not concern technical definitions or product lists, but instead are an issue of the user's intent when deploying widely available cybersecurity technologies. Unfortunately, the Department of State, as the lead U.S. negotiator at Wassenaar, has repeatedly rebuffed industry concerns on this point, saying the *intent* issue is not up for debate. As such, we see no other alternative than for the U.S. government to return to Wassenaar and renegotiate the underlying and overly broad control that was agreed to in 2013.

It is important to recognize however that Congress understood the importance of this issue from the start, with some of you even submitting your strong concerns through the formal DoC rulemaking process back in July. Moreover, Symantec wishes to thank many of you here today for your leadership in sending a letter last month to the President's National Security Advisor urging the Administration to send the export control rule back to Wassenaar to be renegotiated or heavily revised.<sup>1</sup> Spearheaded by Congressional Cyber Security Caucus Co-chairs Michael McCaul (R-TX) and Jim Langevin (D-RI), the bipartisan letter was signed by 125 Members of Congress and rightly recognizes that the proposed cybersecurity export control regulations will have a chilling effect on research and innovation, as well as negatively impact the overall cybersecurity posture of the U.S.

## **II. Consequences for Cybersecurity Tools, Testing, Research and Information Sharing**

To understand how the proposed rule will harm cybersecurity, it is necessary to understand how common security products and tools work, the technology they are based on, and how the information generated by them is used. Symantec and the larger cybersecurity industry have serious concerns with the ambiguous and overbroad language used in the proposed rule. That language would capture not only cybersecurity products, but also basic software development and security techniques.

Of note, the rule does not specifically control actual "intrusion" software, reportedly so as not to cause victims of cyber hacking whose electronic devices may be carrying intrusion software without their knowledge to commit inadvertent export control violations. Since "intrusion" software is not itself controlled, proponents and the DoC have said the transfer of exploit samples, proofs of concept, and other forms of malware are not controlled. In reality, however, the controlling systems and technology designed to operate, deliver, and communicate with the "intrusion" software effectively sweeps the entire cybersecurity industry – including all penetration testing systems and virtually all other cybersecurity products such as anti-virus software – into the controls.

Unfortunately, it is not possible to 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. In other words, it is impossible to separate out security software common functionality. Thus, most security technologies end up being swept in for categorical inclusion.

---

<sup>1</sup> [https://langevin.house.gov/sites/langevin.house.gov/files/documents/12-16-15\\_Langevin-McCaul\\_Wassenaar\\_Letter.pdf](https://langevin.house.gov/sites/langevin.house.gov/files/documents/12-16-15_Langevin-McCaul_Wassenaar_Letter.pdf)

### Vulnerability Testing and Patching

Vulnerability testing and patching are examples of how the proposed U.S. rule would put controls on legitimate intrusion software. The DoC has stated that vulnerability scanners, which find potential vulnerabilities in a system without actually exploiting them and extracting data, would not be controlled. But this ignores the reality of the process of vulnerability research, which is not just about finding potential vulnerabilities or even sharing proofs of concept. When finding vulnerabilities and reporting them, the most valuable information is often about how the vulnerability can be exploited and how those exploits work, including the technology used to develop them. This information 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. The DoC states that it 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. The DoC also recognizes that the tools used to test vulnerabilities (which find vulnerabilities and extract data to prove the vulnerability exists) would also meet the technical description of items that fall within the control list.

### Penetration Testing

Controls under the proposed U.S. rule would capture another common and critical set of tools and technology 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. It is also used to evaluate the security of a system or software product by analyzing its weaknesses and attempting to compromise it. The testing 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 are usually three types of 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 look into 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 strictly guarded and not allowed outside of the network – or into the “wild”. While this testing is directed at the target company’s internal networks and systems, often times vulnerabilities in third party hardware and software used in the target’s IT environment are also discovered. When these vulnerabilities are discovered, the testers must notify the developer of the vulnerable product and work with them to develop an effective 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.

### Third Party Software Updates and Patching

Similarly, third parties often engineer “exploits” to provide update services and manual patching for commonly-used software products manufactured 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 with critical infrastructure. Thus, not all exploits are malicious. 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. 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 updating and patching tools that deliver and communicate with the components that apply the security patch.

### Presumption of Denial for Licenses for Rootkits and Zero Day Exploits

Another potentially negative impact of the proposed DoC implementation of the rule on the cybersecurity industry and our customers is the rule’s presumption of denial for all licenses related to “rootkit” and “zero-day” exploit capabilities. In the preamble to the U.S. 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 rootkit and zero-day exploit functionality is highly problematic. First, the policy would limit the development and delivery of defenses for the most dangerous vulnerabilities, zero-days. Zero-day vulnerabilities are previously unknown and unpatched vulnerabilities and make up the majority of what is discovered during penetration testing. In fact, many cybersecurity companies have zero-day focus groups, which specifically research these types of vulnerabilities and proactively exchange information about their exploitability with other vendors and/or manufacturers to help devise an effective 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 from being shared with knowledgeable employees or outside experts, some of whom will inevitably be foreign nationals. If a company is prevented from closing a known vulnerability, the security of its customers and its own networks and products will be put at much greater risk, as cyber criminals are quick to act on these.

The presumptive denial for rootkits is similarly problematic. 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 as intended.

If this common definition is how the DoC 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. Modern security modules often use “rootkit-like” functionality to integrate into the existing code of the operating system; and in doing so change the behavior of the operating system. This is known as “hooking into” an operating system. As such, a fundamental part of most security vendors’ endpoint protection products are “rootkit” capabilities. For instance, when you install Symantec’s Enterprise or Norton security products, 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 identifies a threat—all operating in the background once installed on a device. These “rootkit” capabilities are used in these products because they are the most effective means of accessing the system to monitor for and catch malicious traffic before it can fully infect the system.

“Rootkit” capabilities also are a common function of legitimate software, not just for cybersecurity. Examples include remote control software used by help desk technicians, system administration tools, technical support, and even anti-cheat mechanisms for video games. These types of software programs with “rootkit capabilities” are not malicious, but the proposed rule does not distinguish between those used with a system administrator’s or user’s knowledge, and those put there by a malicious actor. In light of the broad range of legitimate uses for “rootkit” capabilities, a policy of presumptive denial is clearly inappropriate and does not account for how security software is designed for interoperability.

Simply put, not every rootkit or zero-day is shared or used for malicious purposes – the cybersecurity industry uses these same exploits in order to fix dangerous vulnerabilities. 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 a company and its suppliers will severely impact the ability to create safe products and ensure a secure network and IT environment.

Further, 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.

### Real-Time Information Sharing

The cyber threats we face every day are growing in both numbers and sophistication. Over the last three years we have seen more than *one billion* identities exposed through breaches. Sensitive trade secrets and intellectual property are being pilfered at an unprecedented rate. As detailed in Symantec’s 2015 Internet Security Threat Report, the use of malware is growing and becoming more sophisticated, with nearly *one million* new variants released every day.<sup>2</sup> Attackers are constantly evolving and honing their capabilities to avoid detection, and there are a broad set of tools available to them.

Vulnerabilities continue to be a big part of the security picture, where operating system and other patches have been critical to helping keep systems secure. For example, in April 2014, the discovery of vulnerabilities such as Heartbleed and ShellShock, and their widespread prevalence across multiple operating systems exposed millions of consumers and businesses worldwide to attack. These vulnerabilities existed in the underlying web authentication protocols (SSL and TLS) and given the seriousness, created a global call to action for companies, researchers and governments. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a massive surge of attacks, and cybersecurity professionals around the world mobilized to coordinate and respond.

This is the exact type of urgent and necessary global collaboration that would be impractical and severely hindered under the U.S. rule where we would be required to apply for and wait for an export license before discussing such vulnerabilities with non-U.S. nationals. Compounding the issue is that even if all parties applied for an export license to be able to share such information, that request would be presumptively denied under the current U.S. rule.

---

<sup>2</sup> Symantec Internet Security Threat Report, April 2015.  
[http://www.symantec.com/security\\_response/publications/threatreport.jsp](http://www.symantec.com/security_response/publications/threatreport.jsp)

Another area that would be impacted is information sharing with global law enforcement and government agencies. Today, Symantec shares cyber threat information with international cyber response organizations and law enforcement entities around the world, including INTERPOL, EUROPOL, and national CERTs and cyber police agencies. This work often extends to specific global cybercrime cases, such as botnet eradication and criminal prosecutions.

For example, in February of 2015, Symantec and other industry players partnered with EUROPOL, the FBI and other national law enforcement agencies in an operation to disable the infrastructure controlling the *Ramnit* botnet and the criminal gang that operated it. *Ramnit* harvested banking credentials from its victims and had infected more than 3.2 million computers across the globe.<sup>3</sup> It is a fact that cybercriminals do not recognize national borders when they commit crimes. However, under the U.S. proposed rule, we could be required to seek a license every time we wanted to share threat information across borders with international law enforcement, severely limiting the successful public-private partnerships we have had to date.

Further, as a global cybersecurity company, Symantec has researchers, engineers and analysts in our operations centers around the world. Under the current U.S. rule, our American employees working in the U.S. would be required to first obtain a government license if they were going to engage in anything more than a cursory conversation about new security vulnerabilities or exploits with any co-worker who is either not a U.S. citizen or who is located outside the U.S. (even if that foreign-based employee was a U.S. citizen). Further, if our U.S. researchers discovered a zero-day vulnerability in one of our non-U.S. customer's products or systems, and we wanted to share that information with the customer, again we would be required to obtain an export license.

In addition, the rule does not envision the accommodation of real-time machine-to-machine information sharing across borders – a function that modern security analytics, detection and protections heavily rely on today. At a time when cyber threats are increasing, it is critical that sharing of cyber threat information – whether by humans or machines – remains unfettered. Long a priority for the Congress and the Administration and as seen in the recently enacted law, cyber threat information sharing would suffer under this export control.

The simple fact is that the rule will do little to stop the spread of malicious intrusion and surveillance tools, or curtail illicit hacking and intrusions in any way. In fact, the current rule would do just the opposite – handcuff security vendors and multinational companies from using all the tools available to them, while imposing no restrictions on cyber criminals.

### **III. Other Critical Infrastructure Sectors Affected by the Rule**

The proposed rule would have severe impacts beyond just the cybersecurity industry as other critical infrastructure sectors and academia would also be required to obtain export licenses for the use and deployment of these tools. Certain industries are legally required to conduct penetration testing, and some have implemented this type of testing as part of their industry standards and best practices, including the financial services, electricity, and healthcare industries.

Under the proposed rule, companies using testing tools and processes to comply with regulatory requirements and industry standards for their networks or facilities outside the U.S. also will need to implement costly and time-consuming changes to their internal compliance programs to obtain export licenses. The consequences of the delays created will undermine existing industry standards and regulations, weaken security, and lead to more frequent security breaches across critical infrastructure sectors.

---

<sup>3</sup> <http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation>

The financial services industry has its own, 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. Under the rule, any multinational U.S. financial institution would be required to seek an export license before testing its own networks. As the Financial Services Roundtable/BITS made clear in its formal comments to the DoC, the proposed rule would “seriously diminish the financial industry’s ability to effectively run day-to-day cybersecurity assurance programs.”<sup>4</sup>

The power industry is another critical infrastructure sector that is required to conduct penetration testing. As part of the North American Electric Reliability Corporation (NERC) CIP standards, cybersecurity is recognized as a critical factor in protecting the nation’s electric grid. Similarly, the healthcare industry has heightened privacy and security concerns associated with the electronic transmission of health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened civil and criminal penalties for breaches and non-compliance with HIPAA standards. By restricting the necessary cybersecurity tools to test overseas networks and products, the rule will make compliance with such requirements more difficult for U.S. multinational companies.<sup>5</sup>

Information sharing would also be an issue for the critical infrastructure sectors. The Financial Services ISAC and the Energy ISAC, both with successful information sharing programs among their company members, also would likely be required to obtain export licenses in order to conduct their business across borders. In addition, in the healthcare sector, one could imagine a scenario where a U.S. multinational healthcare device manufacturer discovers a life-critical, zero-day vulnerability in a product. Under the U.S. rule, the company would be prohibited from sharing details with its experts – or even its customers – around the world while it waits for weeks or months to obtain an export license. Meanwhile, the vulnerability would sit unfixed and open for attack during that time.

#### **IV. Economic Impacts for Industry and Government**

U.S. companies design, test and deploy much of the world’s leading security technology. The U.S. is also home to most of the world’s cybersecurity companies, holding the number one provider position in the global market – which topped \$75 billion in 2015 and could reach \$170 billion by 2020.<sup>6</sup> The proposed rule will have a disproportionate effect on the U.S. cybersecurity industry, because most of the companies are based here. In addition to the economic effects on the cybersecurity industry, the rule would also lead to less secure networks and make them easier prey for cybercriminals. While estimates vary, cybercrime experts have put the annual global cost of cybercrime at \$400 billion or more.<sup>7</sup> Without the benefit of cutting edge research and security available to consumers and companies, this number could rise significantly.

Companies implementing the new rule will surely feel the financial impacts as significant new legal and compliance resources will be needed just to manage this one regulation. At Symantec, our preliminary assessment showed that initially we would need approximately one thousand new licenses, but the actual number could go much higher. This is in comparison to our current annual filings that number less than a dozen. Equally as important, the new regulations would require us to significantly alter our trade compliance program. These changes would result in the hiring of additional compliance personnel and a six-month lead time to collect the information necessary to submit any new export license

---

<sup>4</sup> <http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0231>

<sup>5</sup> <http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0209>

<sup>6</sup> <http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html>

<sup>7</sup> [http://csis.org/files/attachments/140609\\_rp\\_economic\\_impact\\_cybercrime\\_report.pdf](http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf)

requests. The added burdens would impede Symantec's ability to be nimble and agile in responding to real-time threats and cyber attacks.

Further, it is not clear how we would even write a license application given the fact that our penetration testing processes 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 weeks or months for another export license. In the meantime, our networks could remain vulnerable, or our product development and security protection release cycles would be significantly delayed. Both of these would have substantial financial and market impacts on our business. We envisage that most other companies would incur similar economic impacts.

There are also implications for cybersecurity start-ups and small businesses who do not have the compliance programs that large companies have, or know how to deal with these rules. By placing such a heavy compliance burden on small innovators, the likely end result is that the U.S. will drive the cybersecurity industry offshore as the U.S. system will be too complex and resource intensive. When combined with a more stringent U.S. implementation than other nations, start-ups will be even more competitively disadvantaged.

On the government side, the proposed rule represents an unknown but significant licensing burden for the DoC Bureau of Industry and Security (BIS) that is responsible for managing the U.S. export control regime. The exponential increase in license applications from all industries, coupled with the enforcement needed to ensure compliance, would require significant new taxpayer resources. It is highly unlikely that the BIS, as is currently staffed, has the capacity to evaluate and process such a large volume of new applications.

## **V. International Implementation**

Not only do the proposed Wassenaar controls damage U.S. economic and national security, but they also do not effectively control the very export of the items they are targeting. For one thing, countries that are party to the Wassenaar Arrangement and already implemented the rule have taken vastly different approaches. There are multiple interpretations of the underlying Wassenaar agreement language that have led to confusion and implementation that differs significantly from country to country. It is clear that the requirements under the Wassenaar Arrangement differ significantly from how countries are implementing the rule.

For example, in Japan, the government worked closely with industry and the Center for Information on Security Trade Controls, resulting in broad carve-outs for nearly any conceivable cyber security product, technology, and research. However, in the end and when viewed clearly, this is simply a case where a Wassenaar country has recognized that there is no way to control malicious hacking products and technology without also causing severe damage to the legitimate cybersecurity industry and its customers. Unintentionally, Japan has added to the variations on implementation of the control, which inevitability will hold up multinational companies' testing and development work.

A direct result of this ambiguity occurred last year when Hewlett-Packard (HP) and its Zero Day Initiative declined to participate in an annual hacking contest in Japan. HP's head of threat research, Jewel Timpe, cited Japan's implementation of Wassenaar as the reason, and that the risk associated with the real time transfer of research across borders could not be reconciled by their legal and compliance teams. She said, "It's due to difficulty in handling, defining and getting the licensing in real time that the contest demands. On the ground running the contest, how does one effect transfers and not run afoul of the

arrangement? There was no clear path to do that easily and quickly.”<sup>8</sup> There is no doubt that the same questions and lack of clarity will stifle and impede critical research, sharing, and innovation for the legitimate cybersecurity industry across all of the countries that implement the rule.

In the case of Italy, their implementation is essentially in name only with little to no enforcement mechanism in place. Take for example the Hacking Team, a Milan-based information technology company. The Hacking Team’s public business model was to sell offensive intrusion and surveillance capabilities – the exact technology the Wassenaar Arrangement attempted to target with the new controls. However, the Italian export authorities granted a blanket global license to the Hacking Team allowing them to freely export their products around the world to many of the countries that the Wassenaar rule is trying to prevent from obtaining these tools.

Some companies who make products originally targeted to be controlled under the Wassenaar rule simply move to different jurisdictions to avoid onerous or explicit export controls on their products. The Gamma Group, owner of FinFisher (a type of surveillance software known as spyware) has opened subsidiaries and closed others in a number of EU countries and the British Virgin Islands, at least in part to what appears to avoid export controls. Indeed today, the legal status of the FinFisher product appears to be held by a completely separate entity from Gamma. Yet, they were still seen exhibiting their products at an arms fair in Paris recently.

The signatories to Wassenaar represent roughly 25 percent of the countries in the world. The group excludes many countries with growing cybersecurity industries and capabilities, such as Israel and China. Even if the rule were to be implemented uniformly, 75 percent of the world would not be bound by these regulations, putting those who rigorously implement and enforce the rule at a distinct competitive disadvantage. Moreover, the rule would not have its desired effect because the countries that have been accused of using malicious exploits for espionage or using surveillance software to spy on dissidents will still be able to obtain the controlled technologies from other markets. These technologies are already widespread and ubiquitous, and in many cases they are free on the Internet, so as to be nearly impossible to control.

During extensive international outreach and education regarding the impacts of the Wassenaar rule, some officials in European Union (EU) member nations have expressed a recognition that they may have overreached with the original Wassenaar control. Some have indicated a willingness to revisit the control and explore possible fixes at the upcoming Wassenaar Plenary. Indeed, many technical experts and EU export regulators have expressed concern that controls with no technical parameters or thresholds – such as the intrusion and surveillance software rules – will ultimately undermine the overall intent of the Wassenaar Arrangement if not addressed and corrected.

## **VI. Attempts to Re-write the Proposed U.S. Rule are Unworkable**

As evidenced by the approximately 300 formal comments to the proposed rule, and as discussed in my testimony, a number of serious technical issues have been raised concerning these controls. To its credit, the DoC recognized the validity of these concerns and quickly withdrew the proposed rule in July. In the weeks and months since, industry and government have met multiple times seeking a common understanding of the issues with the rule, and possible ways to redraft it. The conversations that followed were extensive and frank – and ultimately unsuccessful. They failed for a simple, inescapable reason – the 2013 underlying Wassenaar controls are fundamentally flawed.

---

<sup>8</sup> Mimoso, Michael. “Citing Wassenaar, HP Pulls Out of Mobile Pwn2Own,” ThreatPost, September 4, 2015. <https://threatpost.com/citing-wassenaar-hp-pulls-out-of-mobile-pwn2own/114542/>

There have been no suggestions for technical fixes to the language used in these controls because the issues with the rule are not technical. The core problem remains one of “intent”; fixes to technical definitions or product lists will not solve this issue. All multinational companies need to employ tools for computers or networks that have the functional specifications of the control parameters to avoid detection, defeat protective countermeasures, extract data or information, modify system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are the exact hallmarks a malicious attacker's software would have and what an assessment team would hope to replicate. Thus, the issue becomes one of user intent.

Industry's concern, then, with the existence of such a rule is that it is not possible to use a technical description of the “malicious” tools used by malicious actors to distinguish them from the “legitimate” tools used by the cybersecurity industry – they are effectively the same tools – in an attempt to revise or carve-out exceptions that would allow legitimate cybersecurity uses. Therefore, the rule is both over-broad and will be ineffective in that it does not target that which the drafters presumably intended to target – those with malicious intent.

In addition, the use of exceptions by member states to enable a reasonable implementation of the controls leads to fatally flawed inconsistencies across the Wassenaar members. These inconsistencies lead to continuing questions by multinational companies regarding what is, and is not, controlled – creating a significant compliance burden. Moreover, the U.S. implementation creates a significant competitive disadvantage for U.S. companies who are held to a completely different standard than the rest of the member states.

It has proven to be very difficult, if not impossible to develop fair and consistent exceptions allowing unfettered transfers of such things as generic tools, not designed for purposes of “intrusion”, which can also be used to generate, operate, deliver, or communicate with intrusion software. In order to hide from defenders, many new malware packages rely on existing features of complex operating systems to compromise devices and networks. While authorized teams use tools that would be controlled under Wassenaar, the malicious attackers would freely obtain the tools they need from non-commercial hacking sites. More advanced attackers and state-sponsored hackers would even develop their own custom tools – all while the legitimate users who need to develop the tools or use them for protection are limited from obtaining them while they wait weeks or months for their export licenses.

Altering the controls by developing carve-outs and exceptions are impossible to develop, enforce, and consistently apply. Limited exceptions other than defaulting to end use controls would render the controls ineffective. Realistically, the spread of these tools and technology cannot be limited when most if not all of the tools and technology are already available to non-member countries and large non-state criminal organizations. We believe creating carve-outs and exceptions will ultimately stifle innovation into new areas and techniques for cyber security defense, which cannot be predicted.

At the same time, any such list of exceptions would itself quickly become outdated as new cyber security products that do not match these descriptions are developed. And as noted above, any list of exceptions would be inconsistently applied across the Wassenaar states, thus creating uncertainty for multinational entities as to when a control applies and when it does not. Perhaps a better question to ask is whether the Wassenaar export control regime, or any export control regime, is the right approach to use in controlling the spread of malicious hacking tools and technology?

## **VII. Solutions Outside of the Wassenaar Arrangement Construct**

As discussed throughout this testimony, Symantec believes that revising the proposed U.S. rule will not mitigate the negative effects of the original Wassenaar controls. However, there are more effective ways to address the problematic activity that the rule was designed to deter.

For example, the malicious cyber activity that is targeted under this rule could be countered under criminal law statutes that exist today. The U.S. government could dedicate additional resources to the FBI and federal prosecutors. Over the last decade the FBI and the Department of Justice have developed substantial experience in cyber investigations, forensics, and prosecutions. An export control regime managed by the DoC does not achieve these goals, especially since the technology will still be widely available throughout the world. Malicious cyber attacks are often based overseas, working with abusive foreign governments or underground criminal networks, which are threats that the DoC is neither resourced nor well-suited to address. Ultimately we go back to the fundamental flaw in the proposal – that technology-based export controls are the wrong mechanism to address cybercrime. Controls that are more capable of targeting the ill intent of the people using the software or technology are more suited for this purpose.

Sanctions are another tool that the U.S. government can use to address this threat. The Treasury Department’s Office of Foreign Assets Control (OFAC) is already experienced and heavily engaged in this area. On April 1, 2015, the President issued Executive Order (EO) 13694 titled: *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*. Its purpose is to “enable the U.S. government to block the property and assets of extraterritorial actors involved in cyber attacks, who have otherwise been difficult to reach.”<sup>9</sup> These cyber-enabled activities occurring outside the U.S. may constitute a significant threat to the “national security, foreign policy, or economic health or financial stability of the U.S.” The Treasury Department’s OFAC could dedicate more resources to carry out the EO and serve as a stronger global deterrent to malicious cyber actors. While OFAC just issued regulations implementing the EO last week, to date no designations have been issued.<sup>10</sup>

## Conclusion

Since the U.S. cybersecurity export regulation was proposed in May of 2015, Symantec – together with a broader coalition of the cybersecurity industry and from across the critical infrastructure sectors – has engaged with the Administration about the significant negative consequences and dangers that this new export control regime will bring.<sup>11</sup> While many in the Administration have been receptive to our concerns, including the DoC and DHS, others have held steadfast to a position that ignores the realities of today’s global cybersecurity ecosystem.

As described throughout my testimony, to implement the proposed U.S. regulation, or any variation of the underlying Wassenaar cyber rule, would have catastrophic effects on the cybersecurity industry, multinational corporations that rely on these technologies, and U.S. economic and national security. Any controls in this area should be focused on the intended use, rather than this widely-used technology upon which the world depends. The U.S. government should seek to utilize other authorities and mechanisms as described above to address this issue.

At a time when global cyber threats are increasing every day, it is imperative that the private sector and academia be able to conduct research and provide citizens, businesses, and governments with cutting-edge security products to keep pace with the growing threat. This is no time to restrict the availability of security tools and our ability to share information for cybersecurity purposes.

Symantec strongly recommends that the rule be remanded back to Wassenaar to be renegotiated and more narrowly defined. We look forward to continuing to work with the U.S. government and sharing our technical expertise to achieve an outcome that benefits cybersecurity in the U.S. and around the world.

---

<sup>9</sup> Perkins Coie, April, 2015. <http://www.jdsupra.com/legalnews/president-issues-executive-order-to-bloc-76757/>

<sup>10</sup> Steptoe & Johnson, LLP, January 7, 2016. “OFAC Issues Cyber-Related Sanctions Regulations.” <http://www.steptoelaw.com/publications-10990.html>

<sup>11</sup> Coalition for Responsible Cybersecurity, <http://www.responsiblecybersecurity.org>



**Cheri F. McGuire**  
**Vice President, Global Government Affairs & Cybersecurity Policy**  
**Symantec Corporation**

Ms. Cheri McGuire serves as Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. With twenty five years of government and industry experience, Ms. McGuire is responsible for Symantec’s global public policy agenda and government engagement strategy that includes cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. She leads a team of professionals spanning the United States, Canada, Europe and Asia, and represents the company in key public policy initiatives.

Ms. McGuire works extensively with industry and government organizations. She currently serves on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of The George Washington University Center for Cyber and Homeland Security, the Information Technology Industry Council, and the National Cyber Security Alliance. From 2010 to 2012, she served as Chair of the US IT Sector Coordinating Council – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. She also is a past board member of the IT Information Sharing and Analysis Center, and a former member of the Industry Executive Subcommittee of the President’s National Security Telecommunications Advisory Committee.

Ms. McGuire is a frequent presenter on technology policy issues, including testifying numerous times before the US Congress on cybersecurity, privacy and cybercrime. In addition, she was a speaker at the 2015 Hague Global Conference on Cyberspace, the 2013 Seoul International Cyberspace Conference, the 2012 Budapest Conference on Cyberspace, the United Nations Economic and Social Council plenary session on cybersecurity and development in 2011, and the International Telecommunication Union (ITU) Plenipotentiary special session on cybersecurity in 2010.

Prior to joining Symantec in 2010, Ms. McGuire served as Director for Critical Infrastructure and Cybersecurity in Microsoft’s Trustworthy Computing Group. From 2005 to 2008, she served in numerous positions at DHS, including as Acting Director and Deputy Director of the National Cyber Security Division and US-CERT. In this capacity, she provided leadership for DHS on the Comprehensive National Cybersecurity Initiative (CNCI) released by the President in January 2008, led the implementation of the 2008 National Cyber Exercise – Cyber Storm II, and was Head of US Delegation for bilateral cybersecurity talks with Japan in 2007.

Prior to DHS, she served as a program manager for Booz Allen Hamilton for nearly five years specializing in government telecom and computer security agencies, as a manager for a telecom engineering firm that was acquired by Exelon Infrastructure Services, and as a Congressional staffer for seven years. Ms. McGuire holds an MBA from The George Washington University and a BA from the University of California, Riverside.

**Testimony for the Record**

Iain Mulholland

Vice President, Engineering Trust and Assurance

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform's  
Subcommittee on Information Technology, and the  
Committee on Homeland Security's Subcommittee on  
Cybersecurity, Infrastructure Protection and Security  
Technologies

“Wassenaar: Cybersecurity and Export Control”

January 12, 2016

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Iain Mulholland, head of the Engineering Trust & Assurance Group for VMware. I have nearly 20 years' experience in the product security field, including establishing VMware's Product Security Group in 2011. Before VMware, I worked for a number of leading technology companies, including in 2002, when I was a founding member of the Microsoft Trustworthy Computing Group.

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over \$6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Government; including the Department of Defense, the Civilian agencies, and the Intelligence Community, as well as state and local governments. The company is headquartered in Silicon Valley with 140 offices throughout the world.

VMware is a leading provider of software-defined solutions that make data centers across the globe operate more efficiently and securely and that enable both government and commercial organizations to respond to dynamic business needs in on-premise datacenters, in the cloud, and on personal computers and mobile devices. VMware is providing enhanced security to commercial and government customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers and devices.

### **Concerns with the 2013 Wassenaar Arrangement**

The Wassenaar Arrangement was originally established in order to contribute to regional and international security, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. There are 41 nations, including the U.S., who are part of the Wassenaar Plenary. In order to implement policies from the Wassenaar Arrangement, each participating country has the ability to implement the policies through the application of its national legislation and policies. There is no harmonized implementation across the 41 nations. On May 21, 2015, the Department of Commerce's inter-agency "Bureau of Industry and Security (BIS)" released a draft proposal to implement the 2013 Wassenaar Arrangement. As put forth in the Wassenaar Arrangement, the draft BIS proposal would, in our view, implement much stricter export controls on security technology, including "intrusion software."

The security and protection of our customers is an extremely high priority for VMware and we have made significant investments to proactively ensure the security of our products, services and infrastructure. The 2013 Wassenaar rules would severely impact VMware's ability to test and share code used to test for security vulnerabilities in our products, services and global infrastructure. This would lead to less secure products and in turn, less secure customers. VMware, like many other global U.S. companies, exchanges security-related information across borders as part of its daily operations to conduct research and development, security testing, or address any network breaches

instantaneously, whether it be within our own internal networks, or the networks of our technology partners, business customers, or governments.

Like others in the technology space, we share the concerns about the challenges to be required to apply for and obtain a great number of export licenses to cover the vast range of information-sharing and other security-related activities. This could create a massive backlog and be extremely time-consuming, creating a situation for companies, like VMware, to not be able to share threat information instantaneously and in real-time to prevent or stop a cyber attack on our network, or against the infrastructures of our technology partners, business customers or government. This would only give malicious hackers a window of opportunity to exploit vulnerabilities, knowing that companies like ours would have our hands tied for an extended period of time while applying for and awaiting export licenses to be approved.

The global digital ecosystem is experiencing a level of cyber attacks and sophistication that we have never seen. In order to secure and adequately protect our customers, products, services and networks against these highly sophisticated entities we must utilize every security tool we have in the toolbox.

#### **Examples of how Wassenaar Rules Could Undermine Cyber Posture**

I would like to share for the record some of my personal experiences that I believe speak to the core challenges that implementing the current Wassenaar rules would present not only for VMware as a company, but other similar U.S. companies.

1) In the last 12 months, VMware has collaborated with several small security research organizations in Europe to remediate critical security vulnerabilities they had identified in our products. These vulnerabilities, if left unpatched, could have allowed a malicious attacker to take complete control of critical infrastructure. During the course of the investigation of these issues, the researchers have typically provided VMware with sample exploit code that demonstrated the flaw to VMware's Security Response team. Exploit code is often key in accelerating the speed with which VMware's engineers are able to understand the flaw and develop a patch to protect customers.

In one example the security researcher was in Poland, his parent company was in the Netherlands, the coordinating VMware Incident Response Managers in the US and Canada, and the team responsible for developing the security patch in India. In addition, several of the US-based VMware Security Engineers were non-US persons. In this example, VMware and the Security Researcher would have required multiple export licenses – one from Poland to the Netherlands, one from Poland to the US, one from the Netherlands to the US, one from US to India and several from the US to share information with US-based VMware employees who are not non-US Persons. It is highly unlikely that a researcher based in Poland working for a company based in the Netherlands would have the means or inclination to get multiple export licenses in this scenario and even if they did, this would have introduced delays of many days if not weeks. Furthermore, it is impractical that the individuals charged with leading VMware's response to reports of security vulnerabilities in our products would not be

able to view said reports without first obtaining an export license, nor would they be able to share this information with key team members unless covered by an appropriate export license. In all likelihood, under the proposed Wassenaar rules this flaw would have gone unreported and customers would continue to be vulnerable to this critical security flaw.

In 2015 alone, over half of the security vulnerabilities reported to the VMware Security Response Center from external parties have come from individuals or organizations located in Wassenaar countries. In most cases, an export license would have been required for the party to report the security issue to VMware. A security researcher would likely not even know where they were exporting to since VMware employs security engineers of multiple nationalities in multiple time zones to provide ongoing monitoring for reports of security vulnerabilities in our products. It is highly improbable that these small research companies or individuals will take on the administrative and financial burden of applying for export licenses simply to report security vulnerabilities and as a result, this important source of information will dry up, leaving vulnerabilities unreported and customers less secure.

2) VMware has made a significant investment in the security of our products and we have an established Product Security team that executes a Secure Development Lifecycle (SDL) during the development of our key products. This SDL program is one of the most mature product security programs in the software industry. During the normal course of this SDL, VMware engineers will often develop exploit code to demonstrate security vulnerabilities in our products and services. These exploits are used to test product security, demonstrate that products have been effectively patched, and act as training aids when conducting security training for our global engineering community. These exploits are developed and shared in the course of our daily research and development with engineers across the globe, often with engineers in several different countries and of different nationalities collaborating in real time. As such the ability to develop and rapidly share exploit code within our own engineering community without hindrance is critical to helping ensure the security of VMware products and services.

3) VMware is an active member of a number of software industry product security initiatives including the Software Assurance Forum for Excellence in Code (SAFECode), The Industry Consortium for Advancement of Security on the Internet (ICASI), and the Linux Foundation's Core Infrastructure Initiative. VMware regularly shares security information with participants of these and other forums. Indeed, security is often seen as a leveler and we often share threat information with competitors in an effort to ensure that our mutual ecosystems are protected. For example, in 2014 several significant security vulnerabilities affected major cryptographic implementations. VMware identified that a very commonly used community test for one such vulnerability was inaccurate in how it reported the vulnerable state of certain servers, including a number of VMware server products. The test incorrectly reported that servers were secure when in fact they were not, leading customers into a dangerous false sense of security. Within a matter of hours of the vulnerability becoming known to the community, VMware security engineers released a corrected version of the test, which was in effect a benign exploit, as the vulnerability condition could not be accurately tested at scale in any other

manner. The security community quickly incorporated this corrected test into their frameworks so that customers could correctly assess the security of their infrastructures.

Had we been required to seek an export license in this example, we would have faced a situation where a substantial number of customers initially believed they were secure when they were not, until we were able to release new tests that had the correct export licenses. This situation could have taken many days to resolve instead of being fixed within hours.

With that said, you can see clearly that the 2013 Wassenaar rules, if implemented, will have the exact opposite effect of its intended purpose, meaning it could leave consumers, businesses, and governments less safe from cyber attacks, not more.

### **Next Steps**

Since BIS released its original draft proposal in May, the Department of Commerce and BIS held a series of public forums with stakeholders, ranging from government officials to industry representatives and academics. VMware was pleased to participate in the stakeholder process to work constructively with BIS, the Administration and other stakeholders to find a solution moving forward. BIS should be applauded for their efforts for being transparent with its public forums and working with all stakeholders to better understand the consequences of implementing the 2013 Wassenaar Arrangement.

I would also like to applaud the congressional attention to this issue. In addition to this important congressional hearing, the bipartisan congressional letter spearheaded by Chairman Michael McCaul, Congressman Jim Langevin and signed by over 120 Members of Congress demonstrated the importance for the U.S. to re-think its strategy relating to the 2013 Wassenaar Arrangement.

Moving forward, we recommend that BIS and the Department of Commerce continue to keep all options on the table. This includes two options. The first, we strongly support BIS amending its original draft to reflect some of the concerns raised at its public forum. However, we believe, that even if the U.S. gets its policy right, it still will not be sufficient given the increasing global cybersecurity threats we are facing. That is why, in my opinion, the more effective option is for the U.S. to return to Wassenaar and renegotiate the original 2013 Wassenaar Arrangement dealing with export security controls.

The reality is that VMware, like other global technology companies, not only receives ever-dynamic cyber threat information from inside the U.S., but we also receive a large number from overseas as well. The fact is, with data moving across borders instantly, the cybersecurity ecosystem is not confined to borders. In order to continue to provide world-class secure enterprise software and services and ensure customer safety, we must be able to act on a moment's notice whether that information is coming from the U.S. or abroad. We must have the tools and resources on hand to act immediately.

## **Summary**

We strongly believe that if the 2013 Wassenaar Arrangement is implemented it could undermine our security posture and hinder our ability to adequately protect our customers, products, services and networks. The cyber threats are rapidly changing and are extremely sophisticated. We, collectively as an industry, are charged with providing the world's digital security. To be effective, we will need every tool at our disposal to prevent or mitigate cyber attacks on not only our customers' networks, but our own. The 2013 Wassenaar Arrangement would take away critical tools to counter cyber attacks. It would hinder our ability to prevent or mitigate cyber attacks not only on our customers' networks, but on our own.

We applaud BIS and the Commerce Department for reconsidering its original draft proposal, and hosting a series of public forums with a range of stakeholders to try to find a reasonable solution. Ultimately, however, the U.S. should return to Wassenaar and renegotiate the 2013 Wassenaar Arrangement. We live in a global digital ecosystem. We receive cyber threats against our networks and our customers from all over the world. Even if the U.S. fixes its policy here domestically, it will not enable us to continue to receive critical and timely threat information-sharing from outside our borders.

VMware appreciates the opportunity to share our thoughts on this very important issue. We applaud the leadership and vision of the Chairmen and Ranking Members for holding this hearing. VMware looks forward to continuing to participate in efforts to find solutions to help resolve this issue. Thank you again for the opportunity.

**Committee on Oversight and Government Reform  
Witness Disclosure Requirement – “Truth in Testimony”  
Required by House Rule XI, Clause 2(g)(5)**

Name: **Iain Mulholland**

---

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

**Please see attached supplement.**

---

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

**I am testifying on behalf of VMware, Inc. I am the Vice President for Engineering Trust and Assurance at VMware.**

---

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

**Please see attached supplement.**

---

*I certify that the above information is true and correct.*

Signature:



Date:



Attachment  
 Witness: Ian Mitholland  
 Representing: VMWare, Inc.

Disclosure Form for Witnesses  
 Committee on Oversight and Government Reform  
 U.S. House of Representatives

2015

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
DH153190P0010174	FEDERAL BUREAU OF INVESTIGATION	\$0.00	ADP SOFTWARE
DH153190P0010174	FEDERAL BUREAU OF INVESTIGATION	\$3,811.04	ADP SOFTWARE
HH15233201100186P	PROGRAM SUPPORT CENTER	(\$3,881.00)	OFFICE INFORMATION SYSTEM EQUIPMENT
DH141100P0010702	FEDERAL BUREAU OF INVESTIGATION	(\$40,761)	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL
ITSAC17150040	ITS ACFT1 SERVICE	\$5,085.00	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES
HH15233201200123A	PROGRAM SUPPORT CENTER	(\$6,812.00)	ADP SOFTWARE
AD0278014000040	AGENCY FOR INTERNATIONAL DEVELOPMENT	\$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
ING151X00491	GEOLOGICAL SURVEY	\$12,761.01	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HH15247201500024A	INDIAN HEALTH SERVICE	\$13,804.80	ADP SOFTWARE

2014

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
DH142200P0003969	FEDERAL BUREAU OF INVESTIGATION	(\$299.95)	ADP SOFTWARE
AD0278014000040	AGENCY FOR INTERNATIONAL DEVELOPMENT	\$5,101.16	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
INR14FX00886	BUREAU OF RECLAMATION	\$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HH15247201400106A	INDIAN HEALTH SERVICE	\$12,855.71	ADP SOFTWARE
INR14FX00886	BUREAU OF RECLAMATION	\$24,501.60	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
N666044P3373	DEPT OF THE NAVY	\$1,995.00	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES
CNS1G14P0001	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	\$21,312.06	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
DH141100P0010702	FEDERAL BUREAU OF INVESTIGATION	\$166.60	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL
SS105A11P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	\$409,366.00	ADP SOFTWARE
ST120014N1835	STATE DEPARTMENT OF	\$8,241.00	ADP SOFTWARE
DOL149435567	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	\$9,945.90	ADP SOFTWARE
DH142200P0003969	FEDERAL BUREAU OF INVESTIGATION	\$299.95	ADP SOFTWARE
EP145000021	ENVIRONMENTAL PROTECTION AGENCY	\$15,984.00	IT AND TELECOM- DATA CENTERS AND STORAGE

2013

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
IND14FX00044	OFFICE OF POLICY, MANAGEMENT, AND BUDGET	\$138,965.60	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
M6785409C4762	DEPT OF THE NAVY	\$0.00	IT AND TELECOM- OTHER IT AND TELECOM/COMMUNICATIONS
M6785409C4762	DEPT OF THE NAVY	\$872,065.00	IT AND TELECOM- OTHER IT AND TELECOM/COMMUNICATIONS
AD00CV1300295	AGENCY FOR INTERNATIONAL DEVELOPMENT	\$4,151.00	TRAINING AIDS
SS105A11P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	\$406,064.00	ADP SOFTWARE
CNS1G12P1228	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	\$0.00	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
N0017313P1492	DEPT OF THE NAVY	\$3,296.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
AG3144P130044	USDA, OFFICE OF THE CHIEF FINANCIAL OFFICER	\$6,152.00	EDUCATION/TRAINING- OTHER
FTC13B117	FEDERAL TRADE COMMISSION	\$4,800.00	ADP SOFTWARE
N0016813P3706	DEPT OF THE NAVY	(\$1,875.30)	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
HHNS26320130042	NATIONAL INSTITUTES OF HEALTH	\$4,965.28	ADP SOFTWARE
DOL1494354461	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	\$34,307.30	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HH152002010A1375	CENTERS FOR DISEASE CONTROL AND PREVENTION	\$0.00	ADP COMPONENTS
N0016813P3706	DEPT OF THE NAVY	\$0.00	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
N0016813P3706	DEPT OF THE NAVY	\$3,296.00	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
N0017313P0523	DEPT OF THE NAVY	\$0.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
DOC13G1350108U1	NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION	\$0.00	IT AND TELECOM- SYSTEMS DEVELOPMENT
N0017313P0523	DEPT OF THE NAVY	\$4,000.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
N0018019P19064	DEPT OF THE NAVY	\$16,754.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
W9101712P0084	DEPT OF THE ARMY	\$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS

## **Iain Mulholland, Vice President Research & Development, VMware**

Iain Mulholland leads VMware's Engineering Trust and Assurance (ETA) group. Formed in early 2015, ETA focuses on ensuring customers continue to trust VMware products & services. ETA is a central engineering function within VMware's Research & Development organization comprising Product Security, a group which Mulholland built starting in 2011, Performance Engineering, Quality Systems and the Trust & Assurance team which focuses on Security Certifications, Software Supply Chain Security and the customer facing communication of VMware Trust & Assurance programs.

Prior to VMware he held senior leadership positions in several security and privacy early stage technology startups. A 20-year veteran of the software security space, Mulholland was an early member of the Microsoft Trustworthy Computing Group, where he led the Microsoft Security Response Center. A former British Army Officer, Mulholland is originally from Belfast, Northern Ireland but now calls Northern California home.

**Statement of**  
**Kevin J. Wolf**  
**Assistant Secretary of Commerce for Export Administration**

**Before the**  
**House Committee on Oversight and Government Reform**  
**Subcommittee on Information Technology**

**And the**  
**House Committee on Homeland Security**  
**Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies**

**January 12, 2016**

Thank you, Chairmen Hurd and Ratcliffe, and Ranking Members Kelly and Richmond.

The Wassenaar Arrangement is a 41-member export control group in which the United States participates. It was established to contribute to regional and international security and stability by promoting greater responsibility in the transfer of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations of such items. Participating States maintain a common control list of items warranting control for these reasons and seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals, and are not diverted to support such capabilities. The list of such items is developed and updated by the Participating States through consensus determinations, generally made at the end of each year.

The U.S. Department of State leads the U.S. delegation to the Wassenaar Arrangement but my agency, the Department of Commerce's Bureau of Industry and Security, is responsible for developing and administering the U.S. regulations – the Export Administration Regulations – that implement U.S. export controls for dual-use and some military items on the Wassenaar control list. Other agencies, primarily the Department of Defense, participate in developing proposed changes to the control list to submit to Wassenaar, deciding whether and which controls to agree to, and reviewing the U.S. regulations to implement controls agreed to by the member states. Commerce also has technical advisory committees composed of private sector experts who provide technical and other advice regarding proposals to the regimes.

In December 2013, Wassenaar approved new export controls on “command and delivery platforms” for “intrusion software” and related technology. Specifically, the entries in Category 4 (Computers) of the Wassenaar dual-use control list would control non-publicly available software (4.D.4.) that generates, operates, delivers, or communicates with “intrusion software.” “Intrusion software” is defined as software designed to covertly gain access to a computer or other networked device and, once inside, to extract or modify data or modify the execution

path of the device to allow the execution of externally provided instructions. Related hardware and technology entries (4.A.5. and 4.E.1.c.) control systems and equipment for generating, operating, delivering, or communication with "intrusion software," and technology for developing "intrusion software." The original proposal for these controls came from another Wassenaar member nation in 2012. Examples of the types of commercial hacking software intended to be captured by this control include those offered by Hacking Team (Italy), Gamma/Fin-Fisher (Germany), and Vupen (France).

The controls were novel in that they were the first foray by a multilateral export control community into the area of offensive cyber tools. The agreed-upon entries covering software intentionally excluded "intrusion software" itself -- that is, certain kinds of malware -- from control because of a general understanding that everyone with a computer or mobile device infected by such malware or "exploits" could become an unwitting "exporter" of it (e.g., by forwarding an infected e-mail to someone in another country). The technology entry, however, imposes controls on non-publicly available technology for the development of such software as well as on technology for the development of the controlled delivery systems.

In beginning the process of drafting the regulation to implement the control, Commerce grew concerned that, despite several exclusions set forth in the definition of "intrusion software," the scope of the controls, particularly the technology controls, might be far broader in scope than originally understood by Commerce and its advisory committees. We particularly became concerned that the Category 4 technology control list entry in the draft regulation -- technology for the development of "intrusion software" -- could inadvertently significantly harm both U.S. government and U.S. private sector cybersecurity programs and efforts if implemented.

In order to not take an action that would inadvertently harm our nation's ability to engage in critical cyber defense and related research work, we decided in May 2015 to take the unprecedented step of publishing these Wassenaar control list entries as a proposed rule, with a request for private sector comments, rather than as a final rule. Our hope was that the private sector comments would give us a better sense for whether the rule would have unintended impacts on our cyber defense and cyber research ecosystems. All dual-use controls have consequences and impose costs on the private sector. That is the nature of controls. This one, however, was different because the impact would be not just on the economic bottom-line of U.S. companies, but on our government's and our nation's ability to share efficiently and quickly the types of technology necessary to conduct cyber defense and related research.

Immediately following publication of the proposed rule, Commerce received questions from U.S. private sector and others in the U.S. Government about the intended scope of the controls. In order to ensure that comments were informed and responsive to the proposed controls set forth in the rule, Commerce published answers to a list of "frequently asked questions" on its website to address what we determined were regular queries in order to encourage more focused and more useful public comments. It was clear from these initial questions that the terminology used in the control list entries and the proposed rule were understood differently by the cybersecurity community than by the export control agencies and the Wassenaar Participating States. By the end of the 60-day comment period, Commerce

had received more than 260 comments, virtually all of them negative. Some commenters took the view that the underlying control at Wassenaar could not be implemented without causing significant harms to cybersecurity. Others made specific recommendations on ways to mitigate many of the concerns. Some praised the underlying objectives of the rule, while nonetheless proposing modifications to the scope of the proposed regulation, such as through license exceptions and definitions, to reduce the impact of unintended consequences.

The negative reactions were repeated by extensive outreach our bureau conducted with the security industry, information security and financial institutions, and government agencies that manage cybersecurity. Outreach included multiple open meetings under the auspices of Commerce's technical advisory committees and extensive discussions with cybersecurity managers in the Federal Government.

Neither the Commerce Department nor the Administration has reached a conclusion about how to respond to the public comments. We are still reviewing and considering them. Importantly, all U.S. Government agencies with expertise and equities in cyber defense research and related work are reviewing the comments and will provide input as a next step, before we make a decision on what to do about the proposed rule. As requested by your committees, I can, however, summarize the essence of the comments – reiterating that the Administration has not come to any final conclusions regarding how to respond to the comments or to the extent to which they are correct technically. The public comments, including presentations at technical advisory committee meetings during the past three months, focus on three main issues.

First, some commenters asserted that the proposed regulation's definition of "intrusion software" is too broad and, as a technical matter, fails. They assert that malware recovery tools would be caught by the entries because they interact with malware to regain control of an infected system, and some defense research tools would be caught because they analyze malware to develop new defensive products. They also assert that products that patch systems or add capabilities to programs would themselves be controlled under these entries because of the way they interact with or manipulate programs. These products are integrated with the hardware (systems, equipment, and components) and are designed to legitimately bypass or defeat protections, modify the standard execution path of software, and access data. According to the commenters, they would often thus be software for the generation, operation, delivery of or communication with "intrusion software" and caught by the new controls.

Second, other commenters contend that the proposed rule to implement the control list entries as written, based on the definition of "intrusion software," would impose a heavy and unnecessary licensing burden on legitimate transactions that contribute to cyber security. Government agencies and private sector cyber security companies routinely test their systems and networks to identify vulnerabilities and, if possible, discover existing malicious attack agents. These companies then provide their clients with threat mitigation tools and strategies. To accomplish this, they use the same tools the controls on intrusion items identify, though their use is authorized by their target. To accomplish their mission, they need to employ tools for computers or networks that have the functional specifications of the control parameters, e.g., avoid detection, defeat protective countermeasures, extract data or information, modify

system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are exactly the characteristics a successful malicious attacker's software would have and what the assessment team's tools need to be able to replicate. During these defensive engagements, members of the assessment team frequently need to create custom scripts (i.e., software programs) to effectively assess the extent of the vulnerabilities by creating exploits, and to determine if a successful attack has taken place or is in progress.

Third, other commenters state that the proposed rule's controls on technology for the development of "intrusion software" could cripple legitimate cybersecurity research. To address cyber threats, technical information must be shared with experts across the globe. In order to identify and quickly counter threats, the cybersecurity industry relies heavily on collaboration with other companies within and outside of the United States, as well as independent experts around the world. Many of these experts are self-taught, have no prior formal relationship with cybersecurity firms, and, in many cases, may be unknown until they discover a new vulnerability. To address a vulnerability, a company must be able to engage in a back-and-forth dialogue with these researchers and experts. Often, the dialogue must include detailed discussion of exactly how a particular vulnerability could be exploited to gain control of a computer; without such discussion it is not possible to evaluate the risk posed by a vulnerability or to fashion an effective and comprehensive defense. Some commenters were concerned that, by subjecting vulnerability research, assessments, and testing to export licensing requirements including classification, screening, and other control elements, the control would limit the ability to fix and patch such vulnerabilities, leading to an overall decrease in the quality of cybersecurity. When vulnerabilities are discovered, they must be reported as soon as possible so that a fix can be developed. This process involves sharing not only the vulnerability and exploit, but also the technical information on how the exploits work, including the technology to develop them.

The commenters had many suggestions regarding how to address their concerns. The Administration will be reviewing all of them and many other ideas for how to address the policy objectives of the control but without unintended collateral harms. As I have said many times in response to questions about the rule, the only thing that is certain about the next step is that we will not be implementing as final the rule that was proposed. In working through this process, we will continue to seek input from those with expertise and equities in cyber security in both the U.S. government and the private sector before deciding in conjunction with its interagency partners what the next step should be. I thus welcome the Subcommittees' inputs and am prepared to answer any questions you may have.

**Statement of  
Vann H. Van Diepen  
Principal Deputy Assistant Secretary  
for International Security and Nonproliferation  
U. S. Department of State**

**Before the**

**House Committee on Oversight and Government Reform  
Subcommittee on Information Technology**

**And the**

**House Committee on Homeland Security  
Subcommittee on Cybersecurity, Infrastructure Protection, and Security  
Technologies**

**January 12, 2016**

Thank you, Chairmen Hurd and Ratcliffe, Ranking Members Kelly and Richmond, and Members of the Committees, for the opportunity to talk to you today about nonproliferation export control efforts in the new area of cyber tools. This is a very challenging area. We hear almost daily about malicious cyber activities that disrupt businesses, compromise privacy, or threaten national security. The 2014 destructive malware attack on Sony Pictures Entertainment and recent high profile intrusions involving the exfiltration of sensitive data from government and private sector computers highlight the kinds of cyber threats we now face. These dangers are only increasing as the tools for carrying out these actions in cyberspace become more widely available and more powerful.

While these cyber tools enable breaches of networks and data for malicious purposes, they can also be used for beneficial purposes, such as identifying vulnerabilities and improving cybersecurity. The private sector and security research community play a critical role in promoting cybersecurity, and it is important that they continue to innovate in this dynamic technological space.

Congress itself has recognized the overall cybersecurity threat that our nation faces, and it has sought to specifically address the dangers posed by the uncontrolled spread of capabilities to carry out malicious activity in cyberspace. In the 2014 National Defense Authorization Act, Congress required the President to develop an integrated policy to control the proliferation of what it termed “cyber weapons” through unilateral and multilateral enforcement activities, financial means, and diplomatic engagement.

To be most effective, export controls should be multilateral; obviously, it is easier to evade just the controls of the United States than those of dozens of countries. The Wassenaar Arrangement has the responsibility for multilateral national security export controls on dual-use items not related to weapons of mass destruction (WMD), such as cyber tools. This 41-country regime was established in 1996 to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms

and related dual-use goods and technologies, thus preventing destabilizing accumulations, including by terrorists.

Over Wassenaar's 20-year history, it has contributed to national and international security by establishing control lists and best practices that have led to its Participating States preventing transfers of arms and sensitive dual-use items to countries and programs of concern. The concerted efforts of its members in controlling the items on its lists, and keeping those lists up to date, is a critical component of U.S. and international security. The Wassenaar control lists, along with those of the WMD and missile nonproliferation regimes, form the backbone of the U.S. dual-use control system.

The United States is a global leader in nonproliferation, including in Wassenaar. We have pressed consistently for controls on a range of dual-use technologies that, when used appropriately, can protect us, but can also be used against us, including things like lasers and sophisticated electronics. When all 41 members, as well as the growing number of non-member countries that adhere unilaterally to Wassenaar controls, work together to control sensitive technologies, we can better keep these items out of the hands of those who would use them against us -- while preserving their use in legitimate trade.

We need to strike the appropriate balance in implementing such controls to promote national security objectives while making sure that the controls' benefits

clearly exceed any commercial or national security costs. Upholding our international export control commitments is central to our ability to get other countries to uphold theirs, not just in Wassenaar but in the WMD and missile control regimes as well.

Recognizing the challenge in implementing the cyber control, the U.S. government took the uncommon step of going through a public notice and comment process. Usually, Wassenaar controls get implemented through a final rule. The U.S. government made this decision because we wanted to give industry and the research community an opportunity to provide their views and wanted to make sure we get U.S. implementation right. The comments were instructive, and we take them very seriously. It is clear from the comments received that the first version of the proposed U.S. rule to implement the Wassenaar control missed the mark, and the interagency continues to work through the concerns raised.

Fortunately, the cyber control is included on the least sensitive portion of the Wassenaar list. This provides us with substantial flexibilities we can employ in the process of implementing that control nationally, just as most other Wassenaar members have done in already having implemented the cyber control for over a year without apparent controversy.

We appreciate your Committees' interests in this issue, and we are committed to working closely with Commerce and all other stakeholders in the

interagency, as well as industry and the other relevant external stakeholders, to seek a balanced way forward that meets our important policy objectives while addressing the concerns raised.