

Docket Content Report

Document ID	Submitter Name	Document Title
BIS-2015-0019-0001		Definitions in the Export Administration Regulations
BIS-2015-0019-0002		Project Harmonization Chart
BIS-2015-0019-0003	Anonymous Kennedy	Comment on FR Doc # 2015-12843
BIS-2015-0019-0004	John DeLallo	Comment on FR Doc # 2015-12843
BIS-2015-0019-0005	David Hendrickson	Comment on FR Doc # 2015-12843
BIS-2015-0019-0006	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0007	John Biltz	Comment on FR Doc # 2015-12843
BIS-2015-0019-0008	mark Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0009	Concerned American	Comment on FR Doc # 2015-12843
BIS-2015-0019-0010	Edward Kosewicz	Comment on FR Doc # 2015-12843
BIS-2015-0019-0011	Neil Sagers	Comment on FR Doc # 2015-12843
BIS-2015-0019-0012	Keith Black	Comment on FR Doc # 2015-12843
BIS-2015-0019-0013	Elizabeth Peloso	University of Pennsylvania
BIS-2015-0019-0014	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0015	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0016	Mark McLellan	Utah State University
BIS-2015-0019-0017	Allen DiPalma	University of Pittsburgh
BIS-2015-0019-0018	Jennifer Lodge	Washington University in St. Louis
BIS-2015-0019-0019	Julie Chen	University of Massachusetts Lowell
BIS-2015-0019-0020	Anonymous Anonymous	Yale University
BIS-2015-0019-0021	Kathleen Palma	General Electric Company
BIS-2015-0019-0022	Krista Campeau	University of Michigan
BIS-2015-0019-0023	Andrew Dean	SABIC Innovative Plastics
BIS-2015-0019-0024	Ara Tahmassian	Harvard University
BIS-2015-0019-0025	Laurel Dean	Ohio State University
BIS-2015-0019-0026	Clint Davis	Comment on FR Doc # 2015-12843

BIS-2015-0019-0027	Shaun Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0028	Sam Schieuer	Comment on FR Doc # 2015-12843
BIS-2015-0019-0029	Thaddeus Warner	Comment on FR Doc # 2015-12843
BIS-2015-0019-0030	Thomas Brewer	Comment on FR Doc # 2015-12843
BIS-2015-0019-0031	Doug Farren	Aerospace Industries Association
BIS-2015-0019-0032	Kelly Hochstetler	University of Virginia
BIS-2015-0019-0033	Matt Watson	Comment on FR Doc # 2015-12843
BIS-2015-0019-0034	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0035	Anonymous Anonymous	Texas A&M
BIS-2015-0019-0036	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0037	Charles Roberts	Comment on FR Doc # 2015-12843
BIS-2015-0019-0038	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0039	Geoffrey Goodale	CEECR - Ad Hoc Coalition for Effective Export Control Reform
BIS-2015-0019-0040	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0041	Jesse Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0042	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0043	Karen Robertson	Intel Corporation
BIS-2015-0019-0044	Jessie Ray	Comment on FR Doc # 2015-12843
BIS-2015-0019-0045	D C	Comment on FR Doc # 2015-12843
BIS-2015-0019-0046	Brian Patriot	Comment on FR Doc # 2015-12843
BIS-2015-0019-0047	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0048	Anonymous Anonymous	Comment on FR Doc # 2015-12843
BIS-2015-0019-0049	James Patrick Briscoe	University of Minnesota
BIS-2015-0019-0050	Christopher Wyngarden	Comment on FR Doc # 2015-12843
BIS-2015-0019-0051		Matthew A. Goldstein, PLLC

BIS-2015-0019-0052		IBM Corporation
BIS-2015-0019-0053		University of Iowa
BIS-2015-0019-0054		University of Rochester
BIS-2015-0019-0055		AAU APLU COGR
BIS-2015-0019-0056		ANS
BIS-2015-0019-0057		ASML US
BIS-2015-0019-0058		AUECO
BIS-2015-0019-0059		SPIE OSA
BIS-2015-0019-0060		K&L Gates LLP
BIS-2015-0019-0061		Brown University
BIS-2015-0019-0062		Cornell University
BIS-2015-0019-0063		Indiana University
BIS-2015-0019-0064		Boeing
BIS-2015-0019-0065		Case Western Reserve University
BIS-2015-0019-0066		Chemours Company
BIS-2015-0019-0067		CISTEC
BIS-2015-0019-0068		University of Chicago
BIS-2015-0019-0069		Alan J. Ramsbotham, Jr.
BIS-2015-0019-0070		SUNY RF
BIS-2015-0019-0071		LORD Corporation
BIS-2015-0019-0072		CompTIA
BIS-2015-0019-0073		Duke University
BIS-2015-0019-0074		University of Idaho
BIS-2015-0019-0075		University of California Research and Graduate Studies
BIS-2015-0019-0076		NYU
BIS-2015-0019-0077		Perspecsys
BIS-2015-0019-0078		University of Wisconsin-Madison
BIS-2015-0019-0079		[University of Michigan -duplicate - see 0022]
BIS-2015-0019-0080		EGAD
BIS-2015-0019-0081		University of Southern California
BIS-2015-0019-0082		Semiconductor Industry Association
BIS-2015-0019-0083		Google
BIS-2015-0019-0084		Lockheed Martin
BIS-2015-0019-0085		UC Berkeley

BIS-2015-0019-0086		Bill Root
BIS-2015-0019-0087		MIT
BIS-2015-0019-0088		National Association of Manufacturers
BIS-2015-0019-0089		University of Colorado - Boulder
BIS-2015-0019-0090		IEEE
BIS-2015-0019-0091		BAE
BIS-2015-0019-0092		Johns Hopkins University
BIS-2015-0019-0093		MIT Lincoln Laboratory
BIS-2015-0019-0094		CPI
BIS-2015-0019-0095		Rockwell Collins
BIS-2015-0019-0096		Texas Tech University
BIS-2015-0019-0097		Vanderbilt University
BIS-2015-0019-0098		Satellite Industry Association
BIS-2015-0019-0099		University of Alabama at Birmingham
BIS-2015-0019-0100		University of Cincinnati
BIS-2015-0019-0101		University of Maryland Baltimore
BIS-2015-0019-0102		United Technologies Corporation

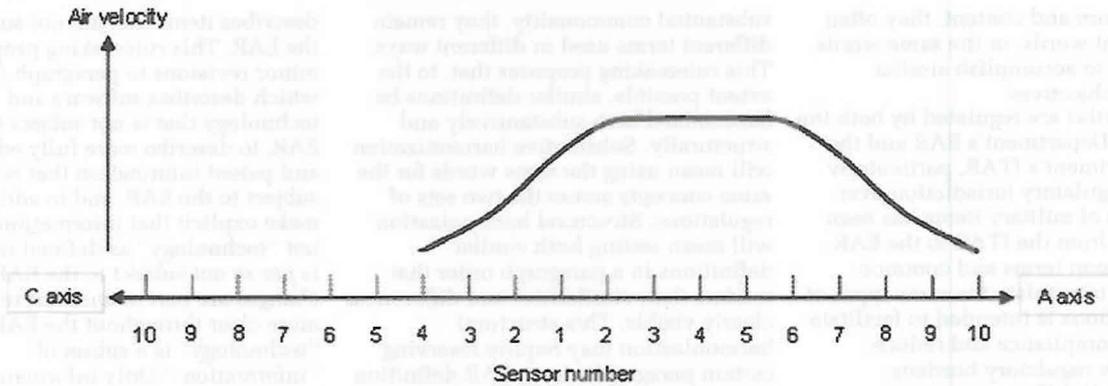


Figure 3: Example Air Velocity Pattern for Airflow Not Directly Downward

[FR Doc. 2015-13169 Filed 6-2-15; 8:45 am]
BILLING CODE 6450-01-P

DEPARTMENT OF COMMERCE

Bureau of Industry and Security

15 CFR Parts 734, 740, 750, 764, and 772

[Docket No. 141016858-5228-01]

RIN 0694-AG32

Revisions to Definitions in the Export Administration Regulations

AGENCY: Bureau of Industry and Security, Commerce.

ACTION: Proposed rule.

SUMMARY: This proposed rule is part of the Administration's Export Control Reform Initiative. The Initiative will enhance U.S. national and economic security, facilitate compliance with export controls, update the controls, and reduce unnecessary regulatory burdens on U.S. exporters. As part of this effort, this rulemaking proposes revisions to the Export Administration Regulations (EAR) to include the definitions of "technology," "required," "peculiarly responsible," "proscribed person," "published," results of "fundamental research," "export," "reexport," "release," "transfer," and "transfer (in-country)" to enhance clarity and consistency with terms also found on the International Traffic in Arms Regulations (ITAR), which is administered by the Department of State, Directorate of Defense Trade Controls (DDTC). This rulemaking also proposes amendments to the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software. DDTC is concurrently

publishing comparable proposed amendments to the ITAR's definitions of "technical data," "required," "peculiarly responsible," "public domain," results of "fundamental research," "export," "reexport," "release," and "retransfer" for the same reasons. Finally, this rulemaking proposes conforming changes to related provisions.

DATES: Comments must be received by August 3, 2015.

ADDRESSES: Comments may be submitted to the Federal rulemaking portal (<http://www.regulations.gov>). The regulations.gov ID for this proposed rule is: [BIS-2015-0019]. Comments may also be submitted via email to publiccomments@bis.doc.gov or on paper to Regulatory Policy Division, Bureau of Industry and Security, Room 2099B, U.S. Department of Commerce, Washington, DC 20230. Please refer to RIN 0694-AG32 in all comments and in the subject line of email comments. All comments (including any personally identifying information) will be made available for public inspection and copying.

FOR FURTHER INFORMATION CONTACT: Hillary Hess, Director, Regulatory Policy Division, Office of Exporter Services, Bureau of Industry and Security at 202-482-2440 or rp2@bis.doc.gov.

SUPPLEMENTARY INFORMATION:

Background

This proposed rule is part of the Administration's Export Control Reform (ECR) Initiative. The Initiative will enhance U.S. national and economic security, facilitate compliance with export controls, update the controls, and reduce unnecessary regulatory burdens on U.S. exporters. As part of this effort, this rulemaking proposes revisions to the Export Administration Regulations (EAR) to include the definitions of

"technology," "required," "peculiarly responsible," "proscribed person," "published," results of "fundamental research," "export," "reexport," "release," "transfer," and "transfer (in-country)" to enhance clarity and ensure consistency with the International Traffic in Arms Regulations (ITAR), which is administered by the Department of State, Directorate of Defense Trade Controls (DDTC). This rulemaking also proposes amendments to the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software. The DDTC is concurrently publishing comparable proposed amendments to the ITAR's definitions of "technical data," "required," "peculiarly responsible," "public domain," results of "fundamental research," "export," "reexport," "release," and "retransfer" for the same reasons. Finally, this rulemaking proposes conforming changes to related provisions.

One aspect of the ECR Initiative includes amending the export control regulations to facilitate enhanced compliance while reducing unnecessary regulatory burdens. For similar national security, foreign policy, including human rights, reasons, the EAR and the ITAR each control, *inter alia*, the export, reexport, and in-country transfer of commodities, products or articles, technology, technical data, software, and services to various destinations, end users, and end uses. The two sets of regulations have been issued pursuant to different statutes, have been administered by different agencies with missions that are distinct from one another in certain respects, and have covered different items (or articles). For those reasons, and because each set of regulations has evolved separately over decades without much coordination between the two agencies regarding

their structure and content, they often use different words, or the same words differently, to accomplish similar regulatory objectives.

Many parties are regulated by both the Commerce Department's EAR and the State Department's ITAR, particularly now that regulatory jurisdiction over many types of military items has been transferred from the ITAR to the EAR. Using common terms and common definitions to regulate the same types of items or actions is intended to facilitate enhanced compliance and reduce unnecessary regulatory burdens. Conversely, if different concerns between the two sets of export control regulations warrant different terms or different controls, then the differences should be clear for the same reason. Such clarity will benefit national security because it will be easier for exporters to know how to comply with the regulations and for prosecutors to be able to prosecute violations of the regulations. Such clarity will also enhance our economic security because it will reduce unnecessary regulatory burdens for exporters when attempting to determine the meaning of key words and phrases across similar sets of regulations. Finally, such harmonization and clarification is a necessary step toward accomplishing one of the ultimate objectives of the ECR initiative, which is the creation of a common export control list and common set of export control regulations.

BIS and DDTTC have identified a series of similar terms in the EAR and the ITAR that are defined differently and that warrant either harmonization or the creation of similar structures that would identify more clearly the differences in how similar concepts are treated under the EAR and the ITAR. The proposed revisions to these terms are generally not intended to materially increase or decrease their existing scope. In particular, BIS and DDTTC will continue to maintain their long-standing positions that "published" (or "public domain") information and the results of "fundamental research" are excluded from the scope of "technology" subject to the EAR and the ITAR's "technical data." Rather, the proposed changes are designed to clarify and update BIS policies and practices with respect to the application of the terms and to allow for their structural harmonization with their counterparts in the ITAR.

Harmonizing definitions does not mean making them identical. For example, under the EAR, technology may be "subject to" or "not subject to the EAR." Technical data under the ITAR is subject to those regulations by definition. While the two terms have

substantial commonality, they remain different terms used in different ways. This rulemaking proposes that, to the extent possible, similar definitions be harmonized both substantively and structurally. Substantive harmonization will mean using the same words for the same concepts across the two sets of regulations. Structural harmonization will mean setting forth similar definitions in a paragraph order that renders their similarities and differences clearly visible. This structural harmonization may require reserving certain paragraphs in an EAR definition if the corresponding paragraph does not exist in the ITAR definition, or vice versa.

A side-by-side comparison on the regulatory text proposed by both Departments is available on both agencies' Web sites: www.pmdtcc.state.gov and www.bis.doc.gov.

Scope of the Export Administration Regulations

An interim rule entitled "Export Administration Regulation; Simplification of Export Administration Regulations" (61 FR 12714) published March 25, 1996, established part 734, Scope of the Export Administration Regulations. The interim rule stated that part 734 "establishes the rules for determining whether commodities, software, technology, software, and activities of U.S. and foreign persons are subject to the EAR." (61 FR at 12716) This rulemaking proposes to streamline and clarify part 734 while retaining its purpose and scope of control.

Items Subject to the EAR

Section 734.2, currently titled "Important EAR terms and principles," contains two sets of important definitions: A definition and description of "subject to the EAR," and definitions of export, reexport, and a number of associated terms. This rulemaking proposes to retitle the section "Subject to the EAR," retain the definition and description of that term, and create separate sections in part 734 to define "export," "reexport," "release," and "transfer (in-country)," which will be described in greater detail below. This rulemaking proposes to remove current § 734.2(b)(7) regarding the listing of foreign territories and possessions in the Commerce Country Chart (Supplement No. 1 to part 738) because it duplicates current § 738.3(b).

Items Not Subject to the EAR

Section 734.3(a) describes items (*i.e.*, commodities, software, or technology) subject to the EAR. Paragraph (b)

describes items that are not subject to the EAR. This rulemaking proposes minor revisions to paragraph (b)(3), which describes software and technology that is not subject to the EAR, to describe more fully educational and patent information that is not subject to the EAR, and to add a note to make explicit that information that is not "technology" as defined in the EAR is *per se* not subject to the EAR. These changes are part of an effort to make more clear throughout the EAR that "technology" is a subset of "information." Only information that is within the scope of the definition of "technology" is subject to the EAR. If information of any sort is not within the scope of the definition of "technology," then it is not subject to the EAR. This proposed rule makes no changes to the notes to paragraphs (b)(2) and (b)(3) that a printed book or other printed material setting forth encryption source code is not itself subject to the EAR, but that encryption source code in electronic form or media remains subject to the EAR. It also makes no changes to the note that publicly available encryption object code software classified under ECCN 5D002 is not subject to the EAR when the corresponding source code meets the criteria specified in § 740.13(e) of the EAR. (See proposed corresponding revisions to § 120.6(b) of the ITAR.)

Published Technology and Software

Current § 734.7 sets forth that technology and software is "published" and thus not subject to the EAR when it becomes generally accessible to the interested public in any form, including through publication, availability at libraries, patents, and distribution or presentation at open gatherings.

This rulemaking proposes a definition of "published" with the same scope but a simpler structure. The proposed § 734.7(a) reads: "Except as set forth in paragraph (b), "technology" or "software" is "published" and is thus not "technology" or "software" subject to the EAR when it is not classified national security information and has been made available to the public without restrictions upon its further dissemination. This proposed definition is substantially the same as the wording of definitions adopted by the multilateral export control regimes of which the United States is a member: The Wassenaar Arrangement, Nuclear Suppliers Group, Missile Technology Control Regime, and Australia Group. The phrase "classified national security information" refers to information that has been classified in accordance with Executive Order 13526, 75 FR 707; 3

CFR 201 Comp., p. 298. The phrasing following the definition quoted above (“such as through”) means that the list that follows consists of representative examples taken from the list of such things that are in both the ITAR and the EAR and merged together. This is not an exhaustive list of published information. Section 734.7(b) keeps certain published encryption software subject to the EAR, a restriction currently found in § 734.7(c). BIS believes that the proposed revised section is easier to read and that the list of examples is easier to update than current text. The relevant restrictions do not include copyright protections or generic property rights in the underlying physical medium. (See proposed corresponding revisions to “public domain” in § 120.11 of the ITAR.)

Fundamental Research

The current § 734.8 excludes most information resulting from fundamental research from the scope of the EAR. The section is organized primarily by locus, specifically by the type of organization in which the research takes place. This proposed rule would revise § 734.8, but it is not intended to change the scope of the current § 734.8. The proposed revisions streamline the section by consolidating different provisions that involve the same criteria with respect to prepublication review, removing reference to locus unless it makes a difference to the jurisdictional status, and adding clarifying notes. The proposed revisions also consistently use the description “arises during or results from fundamental research” to make clear that technology that arises prior to a final result is subject to the EAR unless it otherwise meets the provisions of § 734.8. Comments regarding whether the streamlined § 734.8 text is narrower or broader in scope than the current text in § 734.8 are encouraged.

Proposed notes clarify that technology initially transferred to researchers, *e.g.*, by sponsors, may be subject to EAR, and that software and commodities are not “technology resulting from fundamental research.” Additional notes clarify when technology is “intended to be published,” as it must be in order to be not subject to the EAR pursuant to this section.

Issued in 1985, National Security Decision Directive (NSDD)–189 established a definition of “fundamental research” that has been incorporated into numerous regulations, internal compliance regimes, and guidance documents. Therefore, in this rulemaking, BIS has proposed a definition of “fundamental research”

that is identical to that in NSDD–189. However, BIS solicits comment on a simpler definition that is consistent with NSDD–189, but not identical. Specifically, the alternative definition would read: “‘Fundamental research’ means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.” BIS believes that the scope of this wording is the same as that of the wording in NSDD–189 and seeks comment on whether the final rule should adopt the simpler wording.

The proposed definition of “fundamental research” includes references to “basic” and “applied” research. For clarity, this rulemaking proposes definitions of those terms. The definition of “basic research” in proposed § 734.8 is that currently defined in the EAR (§ 772.1), and in the Wassenaar Arrangement’s General Technology Note as “basic scientific research.” The proposed definition of “applied research” was drawn from the Defense Federal Acquisition Regulation Supplement (48 CFR part 31.205–18). A possible alternative definition of applied research is that found in the 2014 Office of Management and Budget Circular A–11: “Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.” (See proposed corresponding § 120.49 of the ITAR.)

Educational Information

Current § 734.9 states that educational information released by instruction in a catalog course or associated teaching laboratory of an academic institution is not subject to the EAR. This rulemaking proposes moving this exclusion to § 734.3(b) and removing § 734.9. This proposed rule is not intended to change the scope of the current § 734.9.

Patents

This rulemaking proposes to revise current § 734.10, “Patent applications,” for clarity. For example, instead of an internal cross-reference to the section of the EAR identifying items not subject to the EAR the revised section directly states that “technology” is not “subject to the EAR” if it is contained in the patent-related documents described in the section. For the sake of structural consistency with the ITAR’s treatment of information in patents, paragraph (a)(1) is added to state that a patent or an open (published) patent application available from or at any patent office is *per se* not subject to EAR. The proposed revisions do not, however, change the scope of current § 734.10. The existing

footnote to the current § 734.10 is removed because it would be redundant of the proposed text.

Specific National Security Controls

This rulemaking proposes minor conforming edits to current § 734.11, which describes specific national security controls. The proposed revisions do not change the scope of current § 734.11. As described below, this rulemaking proposes to remove Supplement No. 1 to part 734, “Questions and Answers—Technology and Software Subject to the EAR.” Questions and answers are illustrative rather than regulatory and are thus more appropriately posted as Web site guidance than published as regulatory text.

Export

In § 734.2(b) of the current EAR, there are definitions of export, export of technology or software, and export of encryption source code and object code software. Section 772.1 also defines “export” as follows: “Export means an actual shipment or transmission of items out of the United States.” This rulemaking proposes to consolidate the definitions of “export” and “export of technology and software,” while moving “export of encryption source code and object code software” to a new § 734.13.

Proposed § 734.13(a) would have six paragraphs. Paragraphs (a)(4) and (5) would be reserved. The corresponding paragraphs in the ITAR would contain provisions that are not relevant to the EAR.

Proposed paragraph (a)(1) of the definition of “export” uses the EAR terms “actual shipment or transmission out of the United States,” combined with the existing ITAR “sending or taking an item outside the United States in any manner.”

Paragraph (a)(2), specifying the concept of transfer or release of technology to a foreign national in the United States, or “deemed export,” reflects the long-standing BIS practice of treating software source code as technology for deemed export purposes.

Paragraph (a)(3) includes in the definition of “export” transferring by a person in the United States of registration, control, or ownership (i) of a spacecraft subject to the EAR that is not eligible for export under License Exception STA (*i.e.*, spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country, or (ii) of any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country.

Paragraphs (a)(4) and (a)(5) remain reserved, reflecting placeholders. The ITAR's parallel proposed provisions would control transfers to embassies within the United States and defense services. Neither topic is relevant to the EAR.

Paragraph (a)(6) defines as an export the release or other transfer of the means of access to encrypted data. This is intended to complement the exclusion of certain encrypted data from the definition of export, specified in proposed § 734.18(a)(4) and discussed below. Logically, providing the means to decrypt or otherwise access controlled technology or software that is encrypted should constitute a controlled event to the same extent as releasing or otherwise transferring the unencrypted controlled technology or software itself. Upon transfer of the means of access to encrypted technology or software, the technology or software would acquire the classification and control status of the underlying technology or software, as specified in proposed § 764.2(l). The meaning of "clear text" in the proposed definition is no different than an industry standard definition, e.g., information or software that is readable without any additional processing and is not encrypted. Comments are encouraged regarding whether a specific EAR definition of the term is warranted and, if so, what the definition should be.

Paragraph (a)(6) of export and paragraph (a)(4) of reexport in this proposed rule and the DDTC companion proposed rule present different formulations for this control and the agencies request input from the public on which text more clearly describes the control. The agencies intend, however, that the act of providing physical access to unsecured "technical data" (subject to the ITAR) will be a controlled event. The mere act of providing physical access to unsecured "technology" (subject to the EAR) will not, however, be a controlled event unless it is done with "knowledge" that such provision will cause or permit the transfer of controlled "technology" in clear text or "software" to a foreign national.

This provision is not confined to the transfer of cryptographic keys. It includes release or other transfer of passwords, network access codes, software or any other information that the exporter "knows" would result in the unauthorized transfer of controlled technology. As defined in current § 772.1 of the EAR, "knowledge" includes not only positive knowledge that a circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence.

Paragraph (b) of § 734.13 would retain BIS's deemed export rule as set forth in current § 734.2(b). It would also codify a long-standing BIS policy that when technology or source code is released to a foreign national, the export is "deemed" to occur to that person's most recent country of citizenship or permanent residency. See, e.g., 71 FR 30840 (May 31, 2006).

Paragraph (c) would state that items that will transit through a country or countries or will be transhipped in a country or countries to a new country, or are intended for reexport to the new country are deemed to be destined to the new country. This provision would be moved without change from current § 734.2(b)(6).

(See proposed corresponding revisions to § 120.17 of the ITAR.)

Reexport

The current definitions of reexport and reexport of technology or software in § 734.2(b) are shipment or transmission of items from one foreign country to another foreign country, and release of technology or source code to a foreign national "of another country." This rulemaking proposes to move the definition of "reexports" to new § 734.14. In general, the provisions of the proposed definition of reexport parallel those of the proposed definition of export discussed above, except that reexports occur outside of the United States. Paragraphs (a)(1) and (a)(2) mirror the current definition but divide it into two paragraphs so that one paragraph pertains to actual reexports and another paragraph is specific to deemed reexports. Paragraph (a)(3) expands on the existing reference to transfer of registration or operational control over satellites in the definition of reexport in § 772.1 to include transferring by a person outside the United States of registration, control, or ownership (i) of a spacecraft subject to the EAR that is not eligible for reexport under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country, or (ii) of any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country. Paragraph (a)(4) mirrors the proposed addition in the definition of "export" of the concept that releasing or otherwise transferring, in this case, outside the United States, the means to transfer to a foreign national controlled technology or software in readable form constitutes a "reexport." (See proposed corresponding § 120.19 of the ITAR.)

Release

This provision changes the existing definition of "release" in § 734.2(b)(3) and adds it to new § 734.15. Notably, while existing text provides that "visual inspection" by itself constitutes a release of technical data or source code, the proposed text provides that such inspection (including other types of inspection in addition to visual, such as aural or tactile) must actually *reveal* controlled technology or source code. Thus, for example, merely seeing an item briefly is not necessarily sufficient to constitute a release of the technology required, for example, to develop or produce it. This rulemaking proposes adding "written" to current "oral exchanges" as a means of release.

The proposed text also clarifies that the application of "technology" and "software" is a "release" in situations where U.S. persons abroad use personal knowledge or technical experience acquired in the United States in a manner that reveals technology or software to foreign nationals. This clarification makes explicit a long-standing EAR interpretation. This provision complements proposed new § 120.9(a)(5) of the ITAR, which would include in the definition of "defense service" the furnishing of assistance (including training) to the government of a country listed in § 126.1 of the ITAR in the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of a defense article or a part, component, accessory or attachment specially designed for a defense article. The proposed definition does not use the existing phrase "visual inspection by foreign nationals of U.S.-origin equipment and facilities" because such inspections do not *per se* release "technology." For example, merely seeing equipment does not necessarily mean that the seer is able to glean any technology from it and, in any event, not all visible information pertaining to equipment is necessarily "technology" subject to the EAR. (See proposed corresponding § 120.50 of the ITAR.)

Transfer (In-Country)

The current definition of transfer (in-country) is the "shipment, transmission, or release of items subject to the EAR from one person to another person that occurs outside the United States within a single foreign country" (§ 772.1). There is no difference between this phrase and the phrase "in-country transfer" that is used in the EAR. Variations in the use of the term will be harmonized over time.

This proposed rule would remove the definition from § 772.1 and add a revised definition to new § 734.16. This rulemaking proposes: “a transfer (in-country) is a change in end use or end user of an item within the same foreign country.” This revision eliminates any potential ambiguity regarding whether a change in end use or end user within a foreign country is or is not a “transfer (in-country).” This new text would parallel the term “retransfer” in the ITAR. (See proposed corresponding definition of retransfer in § 120.51 of the ITAR.)

Export of Encryption Source Code and Object Code Software

Proposed new § 734.17, export of encryption source code and object code software, would retain the text of § 734.2(b)(9). It would be moved to this section with only minor conforming and clarifying edits so that it is under the section of the regulations that would define when such an “export” occurs rather than under the existing “important EAR terms and principles.” Describing when an export occurs in the “export of encryption source code and object code software” section of the regulations is more clear than under a general “important EAR terms and principles” heading.

Activities That Are Not Exports, Reexports, or Transfers

Proposed new § 734.18 gathers existing EAR exclusions from exports, reexports, and transfers into a single provision, and includes an important new provision pertaining to encrypted technology and software.

Paragraph (a)(1) reflects that by statute, launching a spacecraft, launch vehicle, payload, or other item into space is not an export. See 51 U.S.C. 50919(f).

Paragraph (a)(2), based on existing text in § 734.2(b)(2)(ii), would state that the release in the United States of technology or software to U.S. nationals, permanent residents, or protected individuals is not an export.

Paragraph (a)(3) would move from current § 734.2(b)(8) text stating that shipments between or among the states or possessions of the United States are not “exports” or “reexports.” The word “moving” and “transferring” were inserted next to “shipment” in order to avoid suggesting that the only way movement between or among the states or possessions would not be a controlled event was if they were “shipped.”

Paragraph (a)(4) establishes a specific carve-out from the definition of “export” the transfer of technology and

software that is encrypted in a manner described in the proposed section.

Encrypted information—*i.e.*, information that is not in “clear text”—is not readable, and is therefore useless to unauthorized parties unless and until it is decrypted. As a result, its transfer in encrypted form consistent with the requirements of paragraph (a)(4) poses no threat to national security or other reasons for control and does not constitute an “actual” transmission of “technology” or “software.” Currently, neither the EAR nor the ITAR makes any distinction between encrypted and unencrypted transfers of technology or software for control or definitional purposes.

This section specifies the conditions under which this part of the definition would apply. An important requirement is that the technology or software be encrypted “end-to-end,” a phrase that is defined in paragraph (b). The intent of this requirement is that relevant technology or software is encrypted by the originator and remains encrypted (and thus not readable) until it is decrypted by its intended recipient. Such technology or software would remain encrypted at every point in transit or in storage after it was encrypted by the originator until it was decrypted by the recipient.

BIS understands that end-to-end encryption is not used in all commercial situations, particularly when encryption is provided by third party digital service providers such as cloud SaaS (software as a service) providers and some email services. However, in many such situations, technology or software may be encrypted and decrypted many times before it is finally decrypted and read by the intended recipient. At these points, it is in clear text and is vulnerable to unauthorized release. BIS considered this an unacceptable risk and therefore specified the use of end-to-end encryption as part of the proposed definition. A key requirement of the end-to-end provision is to ensure that no non-US national employee of a domestic cloud service provider or foreign digital third party or cloud service provider can get access to controlled technology or software in unencrypted form.

Paragraph (a)(4)(iii) describes encryption standards for purposes of the definition. In this proposed rule, use of encryption modules certified under the Federal Information Processing Standard 140-2 (FIPS 140-2), supplemented by appropriate software implementation, cryptographic key management and other procedures or controls that are in accordance with guidance provided in current U.S.

National Institute for Standards and Technology publications, would qualify as sufficient security. FIPS 140-2 is a well understood cryptographic standard used for Federal Government procurement in the United States and Canada, as well as for many other uses, both in the United States and abroad. However, BIS understands that companies may use hardware and software that has not been certified by NIST or that does not conform to NIST guidelines (*e.g.*, for internal use or conforming to other standards). To accommodate this, this paragraph allows for use of “similarly effective cryptographic means,” meaning that alternative approaches are allowable provided that they work. In such cases, the exporter is responsible for ensuring that they work. In contrast, the corresponding definition proposed by DDTTC makes FIPS 140-2 conformity a baseline requirement. Hardware and software modules must be certified by NIST, and NIST key management and other implementation standards must be used. Alternatives are not permitted regardless of effectiveness.

This paragraph also specifically excludes from the definition technology and software stored in countries in Country Group D:5 and Russia for foreign policy reasons in light of the embargoes and policies of presumptive denial now in place with respect to such countries.

Logically, providing keys or other information that would allow access to encrypted technology or software should be subject to the same type of controls as the actual export, reexport, or transfer of the technology or software itself. This is specifically addressed in the proposed § 734.13(a)(6) as part of the definition of “export.” In addition, the proposed § 764.2(1) states that for enforcement purposes such an unauthorized release will constitute a violation to the same extent as a violation in connection with the actual export, reexport, or transfer (in-country) of the underlying “technology” or “software.”

Paragraph (c) confirms that the mere ability to access “technology” or “software” while it is encrypted in a manner that satisfies the requirements in the section does not constitute the release or export of such “technology” or “software.” This responds to a common industry question on the issue. (See proposed corresponding § 120.52 of the ITAR.)

Activities That Are Not Deemed Reexports

Proposed § 734.20, activities that are not deemed reexports, merely codifies

BIS's interagency-cleared Deemed Reexport Guidance posted on the BIS Web site dated October 31, 2013. This guidance was created so that the provisions regarding possible deemed reexports contained in §§ 124.16 and 126.18 of the ITAR would be available for EAR technology and source code.

Under this guidance and new § 734.20, release of technology or source code by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport of such technology or source code if the entity is authorized to receive the technology or source code at issue, whether by a license, license exception, or situations where no license is required under the EAR for such technology or source code and the foreign national's most recent country of citizenship or permanent residency is that of a country to which export from the United States of the technology or source code at issue would be authorized by the EAR either under a license exception, or in situations where no license under the EAR would be required.

Release of technology or source code by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport if: (i) The entity is authorized to receive the technology or source code at issue, whether by a license, license exception, or through situations where no license is required under the EAR; (ii) the foreign national is a *bona fide* regular and permanent employee (who is not a proscribed person under U.S. law) directly employed by the entity; (iii) such employee is a national exclusively of a country in Country Group A:5; and (iv) the release of technology or source code takes place entirely within the physical territory of any such country. This rulemaking also proposes a definition of "proscribed person" in § 772.1.

This paragraph corresponds to § 124.16 of the ITAR, but the reference to Country Group A:5 instead of the countries in the corresponding ITAR section varies slightly. This variation is a function of BIS's national security and foreign policy assessment of the application of this proposed rule to the nationals of Country Group A:5 and as part of a general BIS effort to reduce the number of variations in groups of countries identified in the EAR consistent with U.S. national security and foreign policy interests. South Korea and Argentina are in Country Group A:5, but not in ITAR § 124.16.

Malta, Albania, and Cyprus are in § 124.16, but not in Country Group A:5.

For nationals other than those of Country Group A:5 countries, which are close military allies of the United States, other criteria may apply. In particular, the section specifies the situations in which the releases would not constitute deemed exports in a manner consistent with § 126.18 of the ITAR. An additional paragraph on scope of technology licenses included in the Web site would not be included in this proposed § 734.20. It would be included in proposed § 750.7, discussed below. For purposes of this section, "substantive contacts" would have the same meaning as it has in § 126.18 of the ITAR. The proposed phrase "permanent and regular employee" is a combination of BIS's definition of "permanent employee," as set forth in a BIS advisory opinion issued on November 19, 2007, and the ITAR's definition of "regular employee" in § 120.39. This proposed rule adds specific text excluding persons proscribed under U.S. law to make clear that § 734.20 does not authorize release of technology to persons proscribed under U.S. law, such as those on the Entity List or the Specially Designated Nationals List, or persons denied export privileges, and defines "proscribed person" in § 772.1. The US-UK Exchange of Notes and US-Canadian Exchange of Letters referred to in the existing online guidance can be found on the State Department's Web site. The URL's for the letter are not proposed to be published in the EAR since URL addresses periodically change. Upon implementation of a final rule in this regard, BIS will place the URL references in an "FAQ" section of its Web site.

Technology

Like the current definition of "technology" in the EAR (§ 772.1), the definition proposed in this rulemaking is based on the Wassenaar Arrangement definition of technology. It continues to rest on the Wassenaar-defined sub-definitions of "development," "production," and "use," which are currently defined in § 772.1 and which this rulemaking does not propose to change. This rulemaking also does not propose to change BIS's long-standing policy that all six activities in the definition of "use" (operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing) must be present for an item to be classified under an ECCN paragraph that uses "use" to describe the "technology" controlled. See 71 FR 30842, May 31,

2006. The proposed definition includes, as does the current EAR definition, the terms "operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control 'technology') of an item" because such words are used as to describe technology controlled in multiple ECCNs, often with "or" rather than the "and" found in "use."

This rulemaking proposes to incorporate the definitions of "technical data" and "technical assistance" into the definition of "technology" as illustrative lists. The note in the existing definition of "technology" that "technical assistance" "may take the forms such as instruction, skills training, working knowledge, and consulting services" is not repeated given that the proposed definition and its examples would include any "technology" in such circumstances and in a manner that is harmonized with the ITAR's definition of technical data.

This rulemaking proposes to add a note to address a common industry question about modification. This proposed rule also would add three exclusions to clarify the limits of the scope of the definition in a manner consistent with long-standing BIS policy and interpretation of existing scope of "technology." The first two insertions parallel exclusions in the ITAR and the third, the exclusion of telemetry data, mirrors specific exclusions inserted into both the ITAR and the EAR as part of recent changes regarding the scope of U.S. export controls pertaining to satellites and related items. See 79 FR 27417 (May 13, 2014). Several paragraphs of this section are held in reserve merely to allow the entire section to mirror the corresponding ITAR provisions that are not relevant to the EAR. (See proposed corresponding revisions to § 120.10 of the ITAR.)

Questions and Answers—Technology and Software Subject to the EAR

This rulemaking proposes to remove Supplement No. 1 to part 734, "Questions and Answers—Technology and Software Subject to the EAR." Because the questions and answers are illustrative rather than regulatory, they are more appropriately posted as Web site guidance than included in the EAR.

Required

This proposed rule retains the existing EAR definition of "required" in § 772.1, but proposes adding notes clarifying the application of the term. It removes the references in the existing definition to CCL Categories 4, 5, 6, and 9 to avoid the suggestion that BIS

applies the definition of “required” only to the uses of the term in these categories. BIS has never had a separate definition of “required” used elsewhere in the EAR and this removal merely eliminates a potential ambiguity and reflects long-standing BIS policy.

To address common questions BIS has received regarding the meaning of the word “required,” BIS proposes adding two notes to address the questions. The first states that the references to “characteristics” and “functions” are not limited to entries on the CCL that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. It then includes examples of this point. The second refers to the fact that the ITAR and the EAR often divide within each set of regulations or between each set of regulations (a) controls on parts, components, accessories, attachments, and software and (b) controls on the end items, systems, equipment, or other articles into which those parts, components, accessories, attachments, and software are to be installed or incorporated. Moreover, with the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data or “technology” is the same as the jurisdictional status of the defense article or item to which it is directly related. Examples of this point are provided. (See proposed corresponding revisions to § 120.46 of the ITAR.)

Peculiarly Responsible

This rulemaking proposes a definition of the currently undefined term “peculiarly responsible” in order to respond to common industry questions. The new definition would be modeled on the catch-and-release structure BIS adopted for the definition of “specially designed.” Thus, under the proposed definition, an item is “peculiarly responsible” for achieving or exceeding any referenced controlled performance levels, characteristics, or functions if it is used in “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR *unless* (a) the Department of Commerce has determined otherwise in a commodity classification determination, (b) it is identical to information used in or with a commodity or software that is or was in production and is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons, (c) it

was or is being developed for use in or with general purpose commodities or software, or (d) it was or is being developed with “knowledge” that it would be for use in or with commodities or software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software or (ii) exclusively for use in or with EAR99 commodities or software.

Export of Technical Data for U.S. Persons Abroad

This rulemaking proposes to amend the temporary export of technology provisions of existing License Exception TMP by revising § 740.9(a)(3) to clarify that the “U.S. employer” and “U.S. persons or their employees” using this license exception are not foreign subsidiaries. The proposed paragraph streamlines current text without changing the scope. (See proposed corresponding revisions to § 125.4(b)(9) of the ITAR.)

Scope of a License

This proposed revision would implement in the EAR the interagency-agreed boilerplate for all licenses that was posted on the BIS Web site and began appearing on licenses December 8, 2014. It is a slight revision to the existing § 750.7(a), which states that licenses authorize only the transaction(s) described in the license application and the license application support documents. This proposed revision would also codify the existing interpretation that a license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity’s foreign nationals who are permanent and regular employees of the entity’s facility or facilities authorized on the license, except to the extent a license condition limits or prohibits the release of the technology to nationals of specific countries or country groups.

Release of Protected Information

This rulemaking proposes adding a new paragraph (l) to § 764.2 “Violations.” This paragraph would provide that the unauthorized release of decryption keys or other information that would allow access to particular controlled technology or software would, for enforcement purposes, constitute a violation to the same extent as a violation in connection with the export of the underlying controlled “technology” or “software.” Under these and other related provisions, the decryption keys (or other technology), while subject to the EAR, do not themselves retain the classification of the technology that they could

potentially release. This allows them to be secured and transmitted independently of the technology they could be used to release. (See proposed corresponding revisions to § 127.1(b)(4) of the ITAR.)

Removals From and Additions to EAR’s List of Definitions in § 772.1

With the changes proposed in this rulemaking, there would be stand-alone sections in the EAR to address the scope and meaning of “publicly available information,” “publicly available technology and software,” and “technical data.” To avoid redundancy, the existing definitions in § 772.1 would be removed. In light of the changes described above, the definitions of “basic scientific research,” “export,” “reexport,” “required,” “technology,” and “transfer” would be revised accordingly. A clarifying note would be added at the bottom of the definition that the use of “transfer” does not apply to the unrelated “transfers of licenses” provision in § 750.10 or the antiboycott provisions in Supplement No. 8 to part 760 of the EAR. It also states that the term “transfer” may also be included on licenses issued by BIS. In that regard, the changes that can be made to a BIS license are the non-material changes described in § 750.7(c). Any other change to a BIS license without authorization is a violation of the EAR. See §§ 750.7(c) and 764.2(e). Finally, consistent with the explanations above, definitions for the terms “applied research,” “fundamental research,” “peculiarly responsible,” “publicly available encryption software,” “published,” and “release” would be added to § 772.1.

Public Comments

BIS welcomes comments on any aspects of this proposed rule. With respect to the proposed revisions, BIS would like to receive comments that are as specific and well-supported as possible. Particularly helpful comments will include a description of a problem or concern, available data on cost or economic impact, and a proposed solution. BIS also welcomes comments on aspects of this proposed rule that the public considers effective or well designed.

BIS specifically solicits comment on the following issues:

1. Whether the revisions proposed in this rulemaking create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR;
2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted;

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research;

4. Whether the questions and answers in existing Supplement No. 1 to part 734 proposed to be removed by this rulemaking have criteria that should be retained in part 734;

5. With respect to end-to-end encryption described in the proposed revision of the definition of "Activities that are Not Exports, Reexports, or Transfers," whether the illustrative standard proposed in the EAR rulemaking also should be adopted in the ITAR rulemaking; whether the safe harbor standard proposed in the ITAR rulemaking also should be adopted in the EAR rulemaking; or whether the two bodies of regulations should have different standards;

6. Whether encryption standards adequately address data storage and transmission issues with respect to export controls; and

7. Whether the proposed definition of "peculiarly responsible" effectively explains how items may be "required" or "specially designed" for particular functions.

8. The public is asked to comment on the effective date of the final rule. Export Control Reform rules that revised categories of the USML and created new 600 series ECCNs have had a six-month delayed effective date to allow for exporters to update the classification of their items. In general, rules effecting export controls have been effective on the date of publication, due to the impact on national security and foreign policy. As this proposed rule, and the companion proposed rule from the Directorate of Defense Trade Controls, revise definitions within the ITAR and the EAR and do not make any changes to the USML or CCL, a 30-day delayed effective date is proposed to allow exporters to ensure continued compliance.

Export Administration Act

Although the Export Administration Act expired on August 20, 2001, the President, through Executive Order 13222 of August 17, 2001, 3 CFR, 2001 Comp., p. 783 (2002), as amended by Executive Order 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013) and as extended by the Notice of August 7, 2014, 79 FR 46959 (August 11, 2014), has continued the Export Administration Regulations in effect under the International Emergency Economic Powers Act. BIS continues to carry out the provisions of the Export

Administration Act, as appropriate and to the extent permitted by law, pursuant to Executive Order 13222 as amended by Executive Order 13637.

Regulatory Requirements

1. Executive Orders 13563 and 12866 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This proposed rule has been designated a "significant regulatory action," although not economically significant, under section 3(f) of Executive Order 12866. Accordingly, this proposed rule has been reviewed by the Office of Management and Budget (OMB).

2. This proposed rule does not contain information collections subject to the requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) (PRA). Notwithstanding any other provision of law, no person is required to respond to, nor is subject to a penalty for failure to comply with, a collection of information, subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB control number.

3. This proposed rule does not contain policies with Federalism implications as that term is defined under E.O. 13132.

4. Pursuant to the Regulatory Flexibility Act, as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, 5 U.S.C. 601 *et seq.*, BIS has prepared the following initial Regulatory Flexibility Act analysis of the potential impact that this proposed rule, if adopted, would have on small entities.

Description of the Reasons Why Action Is Being Considered

The policy reasons for issuing this proposed rule are discussed in the background section of the preamble of this document, and are not repeated here.

Statement of the Objectives of, and Legal Basis for, the Proposed Rule; Identification of All Relevant Federal Rules Which May Duplicate, Overlap, or Conflict With the Proposed Rule

The objective of this proposed rule (and a proposed rule being published simultaneously by the Department of

State) is to provide greater clarity and precision in the EAR and the ITAR by providing common definitions and common terms to regulate the same types of actions. The proposed rule also seeks to express some concepts more clearly.

The proposed rule would alter definitions in the EAR. It also would update and clarify application of controls to electronically transmitted technology and software.

The legal basis for this proposed rule is 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp., p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013); Notice of August 7, 2014, 79 FR 46959 (August 11, 2014); Notice of November 7, 2014, 79 FR 67035 (November 12, 2014).

No other Federal rules duplicate, overlap, or conflict with this proposed rule.

Number and Description of Small Entities Regulated by the Proposed Action

This proposed rule would apply to all persons engaged in the export, reexport, or transfer of commodities, technology or software that is regulated by the EAR. BIS does not maintain data from which it can determine how many of those persons are small entities as identified in the Small Business Administration size standards. Nevertheless, BIS recognizes that some of those persons are likely to be small entities.

Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Proposed Rule

This proposed rule is unlikely to increase the number of transactions that must be reported to BIS because EAR reporting requirements apply only in five specific situations, none of which would change as a result of this proposed rule. Those situations are: Exports that do not require a license of items on the Wassenaar Arrangement Sensitive List; Exports of High Performance Computers; Exports of certain thermal imaging cameras that do not require a license; Certain exports of Conventional Arms; and 600 series major defense equipment.

Because recordkeeping requirements already apply to all transactions that are subject to the EAR, BIS expects that this proposed rule would not expand recordkeeping requirements.

It is possible that some of these changes would increase the number of

licenses that some small entities would have to seek from BIS although BIS is not aware of any specific instance in which additional licenses would be required.

The following discussion describes the changes that would be made by this proposed rule. It is divided into two sections: Changes that BIS believes would not impose any new regulatory obligations; and Changes that are not intended to impose any new regulatory obligation, but that BIS cannot state with certainty would not do so.

Changes That BIS Believes Would Not Impose Any New Regulatory Burden

This proposed rule would make certain changes to clarify and streamline the definitions of comparable terms, phrases, and concepts between the EAR and the ITAR. Many of these changes are technical in nature and attempt to consolidate and re-phrase the definitions to enhance readability and to parallel the structure of the ITAR's definition of the same term. However, there are a small number of new provisions, but these changes would not impose any new regulatory burdens. Specifically, this proposed rule would make the following changes:

Remove § 734.2(b) which currently defines export, reexport, release, transfer (in country) and export of encryption source code or object code software, because those terms would be defined in separate sections. Section 734.2(b) also states the policy of applying license requirements that apply to a country to its dependencies and possessions; this policy is currently stated elsewhere in the EAR.

Create new separate sections defining export, reexport, release and export of encryption source code or object code software. Those terms would be clarified and presented in a more organized manner, but substantively unchanged from the existing regulatory text.

Create a new section identifying activities that are not exports, reexports, or transfers. This section restates the transactions that are excluded from the definition of export in current regulatory text and adds two additional activities that would be expressly declared not to be exports, reexports or transfers: space launches and sending, taking or storing certain technology or software abroad using specified cryptographic techniques. The former, although not expressly in the current regulatory text, is required by statute (see 51 U.S.C. 50919(f)) and consistent with current BIS practice of not treating a space launch as an export, reexport or transfer. The latter is, in fact, new.

However, by removing the transactions it describes from the definitions of exports, reexports, or transfers, it removes existing license requirements from those transactions.

Clarify without substantively changing the provisions related to patent applications and add specific text stating that technology contained in a patent available from or at any patent office is not subject to the EAR. The addition reflects BIS' long-standing interpretation. To the extent that it could be characterized as new, its only effect would be to appear to release from the EAR technology that some readers of the EAR might have (erroneously) concluded was subject to the EAR.

Add to License Exception TMP text to emphasize that foreign subsidiaries of U.S. companies are neither U.S. employers nor "U.S. persons or their employees" as those terms are used in the license exception. This additional text adds no restriction that is not already imposed by the definition of "U.S. persons" that currently appears in the text of License Exception TMP.

Add text codifying in the EAR limits on transactions authorized by a license that currently are imposed by conditions on the license itself.

Add text prohibiting the release or other transfer of information (e.g., decryption keys, passwords or access codes) with knowledge that such release or other transfer will result in an unauthorized export, reexport or transfer of other technology or software. This addition provides specific grounds for bringing charges with respect to one particular type of misconduct. However, existing EAR provisions, including the prohibition on causing, aiding or abetting a violation of the EAR or license, authorization or order could be used to bring charges for that same type of misconduct.

Changes That Are Not Intended To Impose Any Regulatory Obligation, but That BIS Cannot State With Certainty Would Not Do So

This proposed rule would add definitions for two new terms "applied research," and "peculiarly responsible" and revise the definitions of two existing terms "required" and "transfer (in-country)." It also would adopt BIS' interpretative guidance regarding deemed reexports as regulatory text. These changes are not intended to impose any regulatory obligations on regulated entities, but BIS cannot state with certainty that there will be no impact. This proposed rule would make the following changes:

Add to the existing definition of "fundamental research" a new

definition of "applied research." The information arising from fundamental research is not subject to the EAR. Fundamental research consists of basic and applied research where the results are ordinarily published and shared broadly within the scientific community. This proposed rule would retain the overall concept of fundamental research that is currently in the EAR, but would remove certain limitations based on the type of institution in which the research takes place, relocate the definition of "basic research" from the definitions section of the EAR to the section dealing with fundamental research and provide a definition of applied research.

Add to the EAR a definition of the term "peculiarly responsible." That currently undefined term appears in the definitions of "specially designed" and of "required" in the EAR. This proposed rule would define that term.

Add to the EAR a definition of "proscribed person." This definition does not create any new regulated class. It simply provides a clear, shorthand reference to a person who is already prohibited from receiving items or participating in a transaction that is subject to the EAR without authorization by virtue of U.S. law, such as persons on the Entity List, Specially Designated Nationals, or debarred parties.

Remove from the definition of the term "required" references to CCL Categories 4, 5, 6 and 9 to accurately reflect BIS' long-standing interpretation that its definition applies wherever the EAR imposes a license requirement for technology "required" for a particular process or activity.

In the definition of "transfer (in-country)," replace the phrase "shipment, transmission, or release of items subject to the EAR from one person to another person that occurs outside the United States within a single foreign country" with "a change in end use or end user of an item within the same foreign country." This new text would parallel the term "retransfer" in the ITAR and would eliminate any potential ambiguity that a change in end use or end user within a foreign country is or is not a "transfer (in-country)."

Each of the foregoing changes would serve the overall policy goals of reducing uncertainty and harmonizing the requirements of the ITAR and the EAR. In most instances, reduced uncertainty will be beneficial to persons who have to comply with the regulations, particularly persons who engage in transactions subject to both sets of regulations. They would be able to make decisions more quickly and

have less need to contact BIS for advice. Additionally, by making these terms more explicit, the possibility of their being interpreted contrary to BIS' intent is reduced. Such contrary interpretations would have three undesirable effects. First, they would undermine the national security and foreign policy objectives that the EAR are intended to implement. Second, persons who are interpreting the regulations in a less restrictive manner than BIS intends may seek fewer licenses from BIS than their competitors who are interpreting the regulations consistent with BIS' intent or who are obtaining advice from BIS, thereby gaining a commercial advantage to the detriment of the relevant national security or foreign policy interests. Third, unnecessary regulatory complexity and unnecessary differences between the terminology of the ITAR and that of the EAR could discourage small entities from even attempting to export. The beneficial effects of making these terms more explicit justify any economic impact that might be incurred by small entities that would have to change their conduct because their contrary interpretations could no longer be defended given the clearer and more explicit terms in the regulations.

This proposed rule also would add to the EAR a description of activities that are not deemed reexports. This description currently appears as interpretative guidance on BIS' Web site and closely tracks the regulatory text of the ITAR. Deemed reexports are releases of technology or software source code within a single foreign country by a party located outside the United States to a national of a country other than the country in which the releasing party is located. The guidance describes three situations in which that party may release the technology or source code without obtaining a license from BIS.

By adopting this guidance as regulatory text that closely tracks the text governing the same activities in the ITAR, BIS reduces both complexity and unnecessary differences between the two sets of regulations with the salutary effects of faster decision making, reduced need to contact BIS for advice and reduced possibility that small entities would be discouraged from exporting as noted above.

Description of Any Significant Alternatives to the Proposed Rule That Accomplish the Stated Objectives of Applicable Statutes and That Minimize Any Significant Economic Impact of the Proposed Rule on Small Entities

As required by 5 U.S.C. 603(c), BIS' analysis considered significant

alternatives. Those alternatives are: (1) The preferred alternative of altering definitions and updating and clarifying application of controls to electronically transmitted technology and software; (2) Maintaining the *status quo* and not revising the definitions or updating and clarifying application of controls to electronically transmitted technology and software; and (3) Establishing a size threshold below which entities would not be subject to the changes proposed by this rulemaking.

By altering definitions and updating and clarifying application of controls to electronically transmitted technology and software as this proposed rule would do, BIS would be reducing uncertainty for all parties engaged in transactions that are subject to the EAR. Potential ambiguities would be reduced; decisions could be made more quickly; the need to contact BIS for advice be reduced; and the possibility of inconsistent interpretations providing one party commercial advantages over others would be reduced. Persons (including small entities) engaged in transactions that are subject to the ITAR and transactions that are subject to the EAR would face fewer actual or apparent inconsistencies that must be addressed in their regulatory compliance programs. Although small entities, along with all other parties, would need to become familiar with the revised terminology, in the long run, compliance costs are likely to be reduced when compared to the present situation where the ITAR and the EAR use different terminology to regulate the same types of activity in the same manner. Therefore, BIS adopted this alternative.

If BIS chose to maintain the *status quo*, small entities and other parties would not have to incur the cost and effort of becoming familiar with the revised regulations and any party who is currently interpreting the regulations that would clearly be precluded by the more explicit interpretations would incur the cost of complying with the regulations consistent with their underlying intent and in the way that BIS believes most regulated parties do. However, the benefits of these proposed changes would be lost. Those benefits, greater clarity, consistency between the ITAR and the EAR, and reduced possibility of inconsistent application of the regulations by similarly situated regulated parties, would be foregone. Therefore, BIS has not adopted this alternative.

If BIS chose to create a size threshold exempting small entities as currently defined by the SBA size standards from the changes imposed by this proposed

rule, those entities would face a more complicated regulatory environment than larger entities. The small entities would continue to be subject to the EAR as a whole but without the benefit of the clarifications introduced by this proposed rule. The only way to make a size threshold beneficial to entities falling below the threshold would be to exempt them from all or at least many of the requirements of the EAR. However, doing so would create a major loophole allowing commodities, software, and technology that are controlled for export for national security or foreign policy reasons to go, without restriction, to any party abroad, undermining the interests that the regulations are intended to protect. Therefore, BIS has not adopted this alternative.

List of Subjects

15 CFR Parts 734 and 772

Exports.

15 CFR Parts 740 and 750

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

15 CFR Part 764

Administrative practice and procedure, Exports, Law enforcement, Penalties.

For the reasons stated in the preamble, parts 734, 740, 750, 764, and 772 of the Export Administration Regulations (15 CFR subchapter C) are proposed to be amended as follows:

PART 734—SCOPE OF THE EXPORT ADMINISTRATION REGULATIONS

■ 1. The authority citation for part 734 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 12938, 59 FR 59099, 3 CFR, 1994 Comp., p. 950; E.O. 13020, 61 FR 54079, 3 CFR, 1996 Comp., p. 219; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013); Notice of August 7, 2014, 79 FR 46959 (August 11, 2014); Notice of November 7, 2014, 79 FR 67035 (November 12, 2014).

§ 734.2—[Amended]

■ 2. Section 734.2 is amended by revising the heading to read as follows and by removing and reserving paragraph (b).

§ 734.2 Subject to the EAR.

■ 3. Section 734.3 is amended by revising paragraph (b) introductory text, paragraph (b)(3), the Note to paragraphs (b)(2) and (b)(3), and the Note to paragraph (b)(3) to read as follows.

§ 734.3 Items subject to the EAR.

* * * * *

(b) The following are not subject to the EAR:

* * * * *

(3) Information and “software” that:
(i) Are “published,” as described in § 734.7;

(ii) Arise during, or result from, “fundamental research,” as described in § 734.8;

(iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution; or

(iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order, or are otherwise patent information as described in § 734.10.

Note to paragraphs (b)(2) and (b)(3): A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see § 734.3(b)(2)). However, notwithstanding § 734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see § 734.17). Publicly available encryption object code software classified under ECCN 5D002 is not subject to the EAR when the corresponding source code meets the criteria specified in § 740.13(e) of the EAR.

Note to paragraph (b)(3): Except as set forth in part 760 of this title, information that is not within the scope of the definition of “technology” (see § 772.1 of the EAR) is not subject to the EAR.

* * * * *

■ 4. Section 734.7 is revised to read as follows:

§ 734.7 Published.

(a) Except as set forth in paragraph (b) of this section, unclassified “technology” or “software” is “published,” and is thus not “technology” or “software” subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:

(1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;

(2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;

(3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;

(4) Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the Internet on sites available to the public; or

(5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for publication or presentation.

(b) Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in § 740.13(e) of the EAR.

■ 5. Section 734.8 is revised to read as follows:

§ 734.8 “Technology” that arises during, or results from, fundamental research.

(a) “Technology” that arises during, or results from, fundamental research and is ‘intended to be published’ is thus not “subject to the EAR.”

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technology that arises during or results from fundamental research” except to the extent that such inputs are “technology” that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution or company may decide to restrict or protect the release or publication of “technology” contained in research results. Once a decision is made to maintain such “technology” as restricted or proprietary, the “technology,” if within the scope of § 734.3(a), becomes “subject to the EAR.”

(b) *Prepublication review.* “Technology” that arises during, or results, from fundamental research is “intended to be published” to the extent that the researchers are free to publish the technology contained in the research without restriction or delay.

“Technology” that arises during or results from fundamental research subject to prepublication review is still “intended to be published” when:

(1) Prepublication review is conducted solely to ensure that publication would not compromise patent rights, so long as the review causes no more than a temporary delay in publication of the research results;

(2) Prepublication review is conducted by a sponsor of research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers; or

(3) With respect to research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC), within any appropriate system devised by the agency or the FFRDC to control the release of information by such scientists and engineers.

Note 1 to paragraph (b): Although “technology” arising during or resulting from fundamental research is not considered “intended to be published” if researchers accept restrictions on its publication, such “technology” will nonetheless qualify as “technology” arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Except as provided in § 734.11, “technology” that is subject to other publication restrictions, such as U.S. government-imposed access and dissemination controls, is not “intended to be published.”

(c) *Fundamental research definition.* “Fundamental research” means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) “Basic research” means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) “Applied research” means the effort that:

(i) Normally follows basic research, but may not be severable from the related basic research;

(ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and

(iii) Attempts to advance the state of the art.

§ 734.9 [Removed and Reserved]

■ 6. Section 734.9 is removed and reserved.

■ 7. Section 734.10 is revised to read as follows:

§ 734.10 Patents.

“Technology” is not “subject to the EAR” if it is contained in:

(a) A patent or an open (published) patent application available from or at any patent office;

(b) A published patent or patent application prepared wholly from foreign-origin technology where the application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office;

(c) A patent application, or an amendment, modification, supplement or division of an application, and authorized for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office, 37 CFR part 5; or

(d) A patent application when sent to a foreign country before or within six months after the filing of a United States patent application for the purpose of obtaining the signature of an inventor who was in the United States when the invention was made or who is a co-inventor with a person residing in the United States.

■ 8. Section 734.11 is revised to read as follows:

§ 734.11 Government-sponsored research covered by contract controls.

(a) If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provisions of § 734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific national security controls may nonetheless be made under this provision.

(b) Examples of “specific national security controls” include requirements for prepublication review by the Government, with right to withhold permission for publication; restrictions on prepublication dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research. A general reference to one or more export control laws or regulations or a general reminder that the Government retains the right to classify is not a “specific national security control.”

■ 9. Section 734.13 is added to read as follows:

§ 734.13 Export.

(a) Except as set forth in § 734.17, “export” means:

(1) An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;

(2) Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”);

(3) Transferring by a person in the United States of registration, control, or ownership of:

(i) A spacecraft subject to the EAR that is not eligible for export under License Exception STA (*i.e.*, spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country; or

(ii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country; or

(4) [Reserved]

(5) [Reserved]

(6) Releasing or otherwise transferring decryption keys, network access codes, passwords, “software” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “software” to a foreign national.

(b) Any release in the United States of “technology” or “source code” to a foreign national is a deemed export to the foreign national’s most recent country of citizenship or permanent residency.

(c) The export of an item that will transit through a country or countries or will be transshipped in a country or countries to a new country, or are intended for reexport to the new country, is deemed to be an export to the new country.

■ 10. Section 734.14 is added to read as follows:

§ 734.14 Reexport.

(a) Except as set forth in §§ 734.18 and 734.20, “reexport” means:

(1) An actual shipment or transmission of an item from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;

(2) Releasing or otherwise transferring “technology” or “source code” to a foreign national of a country other than the foreign country where the release or transfer takes place (a “deemed reexport”);

(3) Transferring by a person outside the United States of registration, control, or ownership of:

(i) A spacecraft subject to the EAR that is not eligible for reexport under License Exception STA (*i.e.*, spacecraft that provide space-based logistics,

assembly or servicing of any spacecraft) to a person in or a national of any other country; or

(ii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country; or

(4) Releasing or otherwise transferring outside of the United States decryption keys, network access codes, passwords, “software,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “software” to a foreign national.

(b) Any release outside of the United States of “technology” or “source code” subject to the EAR to a foreign national of another country is a deemed reexport to the foreign national’s most recent country of citizenship or permanent residency, except as described in § 734.20.

(c) The reexport of an item subject to the EAR that will transit through a country or countries or will be transshipped in a country or countries to a new country, or are intended for reexport to the new country, is deemed to be a reexport to the new country.

■ 11. Section 734.15 is added to read as follows:

§ 734.15 Release.

(a) Except as set forth in § 734.18, “technology” and “software” are “released” through:

(1) Visual or other inspection by a foreign national of items that reveals “technology” or “source code” subject to the EAR to a foreign national;

(2) Oral or written exchanges with a foreign national of “technology” in the United States or abroad; or

(3) The application by U.S. persons of “technology” or “software” to situations abroad using personal knowledge or technical experience acquired in the United States, to the extent that the application reveals to a foreign national “technology” or “source code” subject to the EAR.

(b) [Reserved]

■ 12. Section 734.16 is added to read as follows:

§ 734.16 Transfer (in-country).

Except as set forth in § 734.18, a transfer (in-country) is a change in end use or end user of an item within the same foreign country. “Transfer (in-country)” is synonymous with “in-country transfer.”

■ 13. Section 734.17 is added to read as follows:

§ 734.17 Export of encryption source code and object code software.

(a) For purposes of the EAR, the export of encryption source code and object code software means:

(1) An actual shipment, transfer, or transmission out of the United States (see also paragraph (b) of this section); or

(2) A transfer of such software in the United States to an embassy or affiliate of a foreign country.

(b) The export of encryption source code and object code software controlled for “EI” reasons under ECCN 5D002 on the Commerce Control List (see Supplement No. 1 to part 774 of the EAR) includes:

(1) Downloading, or causing the downloading of, such software to locations (including electronic bulletin boards, Internet file transfer protocol, and World Wide Web sites) outside the U.S., or

(2) Making such software available for transfer outside the United States, over wire, cable, radio, electromagnetic, photo optical, photoelectric or other comparable communications facilities accessible to persons outside the United States, including transfers from electronic bulletin boards, Internet file transfer protocol and World Wide Web sites, unless the person making the software available takes precautions adequate to prevent unauthorized transfer of such code. See § 740.13(e) of the EAR for notification requirements for exports or reexports of encryption source code software considered to be publicly available or published consistent with the provisions of § 734.3(b)(3). Publicly available encryption software in object code that corresponds to encryption source code made eligible for License Exception TSU under § 740.13(e) of this subchapter is not subject to the EAR.

(c) Subject to the General Prohibitions described in part 736 of the EAR, such precautions for Internet transfers of products eligible for export under § 740.17(b)(2) of the EAR (encryption software products, certain encryption source code and general purpose encryption toolkits) shall include such measures as:

(1) The access control system, either through automated means or human intervention, checks the address of every system outside of the U.S. or Canada requesting or receiving a transfer and verifies such systems do not have a domain name or Internet address of a foreign government end-user (e.g., “.gov,” “.gouv,” “.mil” or similar addresses);

(2) The access control system provides every requesting or receiving party with notice that the transfer includes or would include cryptographic software subject to export controls under the Export Administration Regulations, and anyone

receiving such a transfer cannot export the software without a license or other authorization; and

(3) Every party requesting or receiving a transfer of such software must acknowledge affirmatively that the software is not intended for use by a government end user, as defined in part 772 of the EAR, and he or she understands the cryptographic software is subject to export controls under the Export Administration Regulations and anyone receiving the transfer cannot export the software without a license or other authorization. BIS will consider acknowledgments in electronic form provided they are adequate to assure legal undertakings similar to written acknowledgments.

■ 14. Section 734.18 is added to read as follows:

§ 734.18 Activities that are not exports, reexports, or transfers.

(a) The following activities are not exports, reexports, or transfers:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space.

(2) While in the United States, releasing technology or software to United States citizens, persons lawfully admitted for permanent residence in the United States, or persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).

(3) Shipping, moving, or transferring items between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, or the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census.

(4) Sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and

(iv) Not stored in a country listed in Country Group D:5 (see Supplement No.

1 to part 740 of the EAR) or in the Russian Federation.

(b) *Definitions.* For purposes of this section, ‘end-to-end encryption’ means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access “technology” or “software” in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such “technology” or “software.”

Note to § 734.18: Releasing “technology” or “software” to any person with knowledge that a violation will occur is prohibited by § 736.2(b)(10) of the EAR.

§ 734.19 [Reserved]

■ 15. Section 734.19 is reserved.

■ 16. Section 734.20 is added to read as follows:

§ 734.20 Activities that are not “deemed reexports.”

(a) Release of “technology” or “source code” by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport of such “technology” or “source code” if:

(1) The entity is authorized to receive the “technology” or “source code” at issue, whether by a license, license exception, or situations where no license is required under the EAR for such “technology” or “source code;” and

(2) The entity is certain that the foreign national’s most recent country of citizenship or permanent residency is that of a country to which export from the United States of the “technology” or “source code” at issue would be authorized by the EAR either under a license exception, or in situations where no license under the EAR would be required.

(b) *Release to A:5 nationals.* Release of “technology” or “source code” by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport of such “technology” or “source code” if:

(1) The entity is authorized to receive the “technology” or “source code” at issue, whether by a license, license exception, or through situations where no license is required under the EAR;

(2) The foreign national is a *bona fide* regular and permanent employee who is not a proscribed person under U.S. law and is directly employed by the entity;

(3) Such employee is a national exclusively of a country in Country Group A:5; and

(4) The release of “technology” or “source code” takes place entirely within the physical territory of any such country.

(c) *Release to other than A:5 nationals.* Release of “technology” or “source code” by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport of such “technology” or “source code” if:

(1) The entity is authorized to receive the “technology” or “source code” at issue, whether by a license, license exception, or situations where no license is required under the EAR;

(2) The foreign national is a *bona fide* regular and permanent employee who is not a proscribed person under U.S. law and is directly employed by the entity;

(3) The release takes place entirely within the physical territory of the country where the entity is located, conducts official business, or operates;

(4) The entity has effective procedures to prevent diversion to destinations, entities, end users, and end uses contrary to the EAR; and

(5) Any one of the following six (*i.e.*, paragraphs (c)(5)(i), (ii), (iii), (iv), (v), or (vi) of this section) situations is applicable:

(i) The foreign national has a security clearance approved by the host nation government of the entity outside the United States;

(ii) The entity outside the United States:

(A) Has in place a process to screen the foreign national employee and to have the employee execute a non-disclosure agreement that provides assurances that the employee will not disclose, transfer, or reexport controlled technology contrary to the EAR;

(B) Screens the employee for substantive contacts with countries listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR). Although nationality does not, in and of itself, prohibit access to “technology” or “source code” subject to the EAR, an employee who has substantive contacts with persons from countries listed in Country Group D:5 shall be presumed to raise a risk of

diversion, unless BIS determines otherwise;

(C) Maintains a technology security or clearance plan that includes procedures for screening employees for such substantive contacts;

(D) Maintains records of such screenings for the longer of five years or the duration of the individual’s employment with the entity; and

(E) Will make such plans and records available to BIS or its agents for civil and criminal law enforcement purposes upon request;

(iii) The entity is a UK entity implementing § 126.18 of the ITAR (22 CFR 126.18) pursuant to the US–UK Exchange of Notes regarding § 126.18 of the ITAR for which the UK has provided appropriate implementation guidance;

(iv) The entity is a Canadian entity implementing § 126.18 of the ITAR pursuant to the US–Canadian Exchange of Letters regarding § 126.18 of the ITAR for which Canada has provided appropriate implementation guidance;

(v) The entity is an Australian entity implementing the exemption at paragraph 3.7b of the ITAR Agreements Guidelines; or

(vi) The entity is a Dutch entity implementing the exemption at paragraph 3.7c of the ITAR Agreements Guidelines.

(d) *Definitions.* (1) “Substantive contacts” includes regular travel to countries in Country Group D:5; recent or continuing contact with agents, brokers, and nationals of such countries; continued demonstrated allegiance to such countries; maintenance of business relationships with persons from such countries; maintenance of a residence in such countries; receiving salary or other continuing monetary compensation from such countries; or acts otherwise indicating a risk of diversion.

(2) “*Permanent and regular employee*” is an individual who:

(a) Is permanently (*i.e.*, for not less than a year) and directly employed by an entity, or

(b) Is a contract employee who: (i) Is in a long-term contractual relationship with the company where the individual works at the entity’s facilities or at locations assigned by the entity (such as a remote site or on travel);

(ii) Works under the entity’s direction and control such that the company must determine the individual’s work schedule and duties;

(iii) Works full time and exclusively for the entity; and

(iv) Executes a nondisclosure certification for the company that he or she will not disclose confidential

information received as part of his or her work for the entity.

Note to paragraph (d)(2): If the contract employee has been seconded to the entity by a staffing agency, then the staffing agency must not have any role in the work the individual performs other than to provide the individual for that work. The staffing agency also must not have access to any controlled “technology” or “source code” other than that authorized by the applicable regulations or a license.

PART 740—LICENSE EXCEPTIONS

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

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

■ 18. Section 740.9(a)(3) is revised to read as follows:

§ 740.9 Temporary imports, exports, reexports, and transfers (in-country) (TMP).

* * * * *

(a) * * *

(3) “Technology,” regardless of media or format, may be exported by or to a U.S. person or a foreign national employee of a U.S. person, traveling or on temporary assignment abroad, subject to the following restrictions:

(i) Foreign nationals may only export or receive such “technology” as they are authorized to receive through a license, license exception other than TMP or because no license is required.

(ii) “Technology” exported under this authorization may only be possessed or used by a U.S. person or authorized foreign national and sufficient security precautions must be taken to prevent the unauthorized release of the “technology.” Such security precautions include encryption of the “technology,” the use of secure network connections, such as Virtual Private Networks, the use of passwords or other access restrictions on the electronic device or media on which the “technology” is stored, and the use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. Government or is directly employed by a U.S. person and not, *e.g.*, by a foreign subsidiary.

(iv) Technology” authorized under this exception may not be used for foreign production purposes or for technical assistance unless authorized through a license or license exception other than TMP.

(v) The U.S. person employer of foreign nationals must document the use of this exception by foreign national

employees, including the reason that the “technology” is needed by the foreign nationals for their temporary business activities abroad on behalf of the U.S. person.

PART 750—APPLICATION PROCESSING, ISSUANCE, AND DENIAL

■ 19. The authority citation for 15 CFR part 750 continues to read as follows:

Authority: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; Sec 1503, Pub. L. 108–11, 117 Stat. 559; E.O. 13026, 61 FR 58767, 3 CFR, 1996 Comp., p. 228; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; E.O. 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013); Presidential Determination 2003–23 of May 7, 2003, 68 FR 26459, May 16, 2003; Notice of August 7, 2014, 79 FR 46959 (August 11, 2014).

■ 20. Section 750.7 is amended by revising paragraph (a) to read as follows:

§ 750.7 Issuance of licenses.

(a) *Scope.* Unless limited by a condition set out in a license, the export, reexport, or transfer (in-country) authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. The applicant must inform the other parties identified on the license, such as the ultimate consignees and end users, of the license’s scope and of the specific conditions applicable to them. BIS grants licenses in reliance on representations of the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted. A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity’s foreign nationals who are permanent and regular employees (and who are not proscribed persons under U.S. law) of the entity’s facility or facilities authorized on the license, except to the extent a license condition limits or prohibits the release of the technology to nationals of specific countries or country groups.

PART 764—ENFORCEMENT AND PROTECTIVE MEASURES

■ 21. The authority citation for part 764 continues to read as follows:

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

■ 22. Section 764.2 is amended by adding paragraph (l) to read as follows:

§ 764.2 Violations.

(l) No person may “release” or otherwise transfer information, such as decryption keys, network access codes, or passwords, that would allow access to other “technology” in clear text or “software” with “knowledge” that the release will result, directly or indirectly, in an unauthorized export, reexport, or transfer of the “technology” in clear text or “software.” Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled “technology” or “software.”

PART 772—DEFINITIONS OF TERMS

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

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

■ 24. Section 772.1 is amended by:

- a. Adding, in alphabetical order, the definition for “Applied research”;
- b. Revising the definitions of “Basic scientific research” and “Export”;
- c. Adding, in alphabetical order, definitions for “Fundamental research,” “Peculiarly responsible,” “Proscribed person,” and “Publicly available encryption software”;
- d. Removing the definitions of “Publicly available information” and “Publicly available technology and software”;
- e. Adding, in alphabetical order, the definition for “Published”;
- f. Revising the definitions of “Reexport”;
- g. Adding, in alphabetical order, the definition for “Release”;
- h. Revising the definition of “Required”;
- i. Removing the definition of “Technical data”; and
- j. Revising the definitions of “Technology,” and “Transfer.”

The revisions and additions read as follows:

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

Applied research. See § 734.8(c) of the EAR.

Basic scientific research. (GTN)—Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective. See also § 734.8(c) of the EAR.

Export. See § 734.13 of the EAR.

Fundamental research. See § 734.8 of the EAR.

Peculiarly responsible. An item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR unless:

(1) The Department of Commerce has determined otherwise in a commodity classification determination;

(2) [Reserved];

(3) It is identical to information used in or with a commodity or software that:

(i) Is or was in production (*i.e.*, not in development); and

(ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(4) It was or is being developed with “knowledge” that it would be for use in or with commodities or software:

(i) Described in an ECCN; and

(ii) Also commodities or software either not enumerated on the CCL or the USML (*e.g.*, EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(5) It was or is being developed for use in or with general purpose commodities or software, *i.e.*, with no “knowledge” that it would be for use in or with a particular commodity or type of commodity; or

(6) It was or is being developed with “knowledge” that it would be for use in or with commodities or software described:

(i) In an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or

(ii) Exclusively for use in or with EAR99 commodities or software.

Proscribed person. A person who is prohibited from receiving the items at issue or participating in a transaction that is subject to the EAR without authorization by virtue of U.S. law, such as persons on the Entity List, Specially Designated Nationals, or debarred parties.

Publicly available encryption software. See § 740.13(e) of the EAR.

Published. See § 734.7 of the EAR.

Reexport. See § 734.14 of the EAR.

Release. See § 734.15 of the EAR.

Required. (General Technology Note)—As applied to “technology” or

“software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such “required” “technology” or “software” may be shared by different products. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Note 1 to the definition of required: The references to “characteristics” and “functions” are not limited to entries on the CCL that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, ECCN 9A610.a controls “military aircraft specially designed for a military use that are not enumerated in USML paragraph VIII(a).” No performance level is identified in the entry, but the control characteristic of the aircraft is that it is specially designed “for military use.” Thus, any technology, regardless of significance, peculiar to making an aircraft “for military use” as opposed to, for example, an aircraft controlled under ECCN 9A991.a, would be technical data “required” for an aircraft specially designed for military use thus controlled under ECCN 9E610.

Note 2 to the definition of required: The ITAR and the EAR often divide within each set of regulations or between each set of regulations:

1. Controls on parts, components, accessories, attachments, and software; and
2. Controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated.

Moreover, with the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data or “technology” is the same as the jurisdictional status of the defense article or “item subject to the EAR” to which it is directly related. Thus, if technology is directly related to the production of a 9A610.x aircraft component that is to be integrated or installed in a USML VIII(a) aircraft, then the technology is controlled under ECCN 9E610, not USML VIII(i).

* * * * *

“Technology” means:

(a) Except as set forth in paragraph (b) of this definition:

- (1) Information necessary for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item. “Technology” may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;

Note to paragraph (a)(1) of this definition: The modification of an existing item creates a new item and technology for the modification is technical data for the development of the new item.

- (2) [Reserved];
 - (3) [Reserved];
 - (4) [Reserved]; or
 - (5) Information, such as decryption keys, network access codes, or passwords, that would allow access to other “technology” in clear text or “software.”
- (b) “Technology” does not include:
- (1) Non-proprietary general system descriptions;
 - (2) Information on basic function or purpose of an item; or
 - (3) Telemetry data as defined in note 2 to Category 9, Product Group E (see Supplement No. 1 to Part 774 of the EAR).

* * * * *

Transfer. A shipment, transmission, or release of items subject to the EAR either within the United States or outside the United States. *For in-country transfer/transfer (in-country)*, see § 734.16 of the EAR.

Note to definition of transfer: This definition of “transfer” does not apply to § 750.10 of the EAR or Supplement No. 8 to part 760 of the EAR. The term “transfer” may also be included on licenses issued by BIS. In that regard, the changes that can be made to a BIS license are the non-material changes described in § 750.7(c) of the EAR. Any other change to a BIS license without authorization is a violation of the EAR. See §§ 750.7(c) and 764.2(e) of the EAR.

* * * * *

Dated: May 18, 2015.
Kevin J. Wolf,
Assistant Secretary for Export Administration.
 [FR Doc. 2015-12843 Filed 6-2-15; 8:45 am]

BILLING CODE P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 558

[Docket No. FDA-2010-N-0155]

Veterinary Feed Directive Regulation Questions and Answers; Draft Guidance for Industry; Availability

AGENCY: Food and Drug Administration, HHS.

ACTION: Draft revised guidance; availability.

SUMMARY: The Food and Drug Administration (FDA) is announcing the availability of a draft revised guidance for industry (GIF) #120 entitled “Veterinary Feed Directive Regulation Questions and Answers.” The purpose of this document is to describe the current Veterinary Feed Directive (VFD) requirements for veterinarians, feed manufacturers and other distributors, animal producers, and other parties involved in the distribution or use of medicated feed containing a veterinary feed directive drug (VFD feed). This draft revised guidance reflects changes to the VFD requirements under the VFD final rule.

DATES: Although you can comment on any guidance at any time (see 21 CFR 10.115(g)(5)), to ensure that the Agency considers your comment on this draft guidance before it begins work on the final version of the guidance, submit either electronic or written comments on the draft guidance by August 3, 2015.

ADDRESSES: Submit written requests for single copies of the guidance to the Policy and Regulations Staff (HFV-6), Center for Veterinary Medicine, Food and Drug Administration, 7519 Standish Pl., Rockville, MD 20855. Send one self-addressed adhesive label to assist that office in processing your requests. See the **SUPPLEMENTARY INFORMATION** section for electronic access to the draft guidance document.

Submit electronic comments on the draft guidance to <http://www.regulations.gov>. Submit written comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852.

FOR FURTHER INFORMATION CONTACT: Dragan Momcilovic, Center for Veterinary Medicine (HFV-226), Food and Drug Administration, 7519 Standish Pl., Rockville, MD 20855, 240-453-6856, dragan.momcilovic@fda.hhs.gov.

SUPPLEMENTARY INFORMATION:

1. Not Subject to the EAR and Defense Article

<p>§734.3 (a) (NO REVISION)</p> <p>(b) The following are not subject to the EAR:</p> <p>(1) (NO REVISION)</p> <p>(2) (NO REVISION)</p> <p>(3) Information and “software” that:</p> <p>(i) Are “published,” as described in § 734.7;</p> <p>(ii) Arise during, or result from, “fundamental research,” as described in § 734.8;</p> <p>(iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution;</p> <p>(iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order, or are otherwise patent information as described in § 734.10.</p>	<p>§120.6 (a) Defense article means any item, software or technical data designated in §121.1 of this subchapter. [Only the first sentence is being revised]</p> <p>(b) The following are not defense articles and thus not subject to the ITAR:</p> <p>(1) Reserved</p> <p>(2) Reserved</p> <p>(3) Information and software that:</p> <p>(i) Are in the public domain, as described in §120.11;</p> <p>(ii) Arise during, or result from, fundamental research, as described in §120.46;</p> <p>(iii) Concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution; or</p> <p>(iv) Appear in patents or open (published) patent applications available from or at any patent office, unless covered by an invention secrecy order.</p>
--	--

Note to paragraphs (b)(2) and (b)(3) of this section: A printed book or other printed material setting forth encryption source code is not itself subject to the EAR (see §734.3(b)(2)). However, notwithstanding §734.3(b)(2), encryption source code in electronic form or media (e.g., computer diskette or CD ROM) remains subject to the EAR (see §734.17). Publicly available encryption object code software classified under ECCN 5D002 is not subject to the EAR when the corresponding source code meets the criteria specified in §740.13(e) of the EAR.

Note to paragraph (b)(3) of this section: Except as set forth in part 760 of this title, information that is not within the scope of the definition of “technology” (see § 772.1 of the EAR) is not subject to the EAR.

Note: Information that is not within the scope of the definition of technical data (see § 120.10 of this subchapter) and not directly related to a defense article, or otherwise described on the USML, is not subject to the ITAR.

2. Technology/Technical Data

<p>§772.1 “Technology” means:</p> <p>(a) Except as set forth in paragraph (b):</p> <p>(1) Information necessary for the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item. “Technology” may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;</p> <p><i>Note to Paragraph (a)(1) of this section: The modification of an existing item creates a new item and technology for the modification is technical data for the development of the new item.</i></p> <p>(2) [Reserved];</p> <p>(3) [Reserved];</p> <p>(4) [Reserved]; or</p>	<p>§120.10 Technical Data</p> <p>(a) Technical data means, except as set forth in (b):</p> <p>(1) Information required for the development (<i>see</i> §120.47) (including design, modification, and integration design), production (<i>see</i> §120.48) (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article. Technical data may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;</p> <p><i>Note 1 to Paragraph (a)(1):</i> The modification of an existing item creates a new item and technical data for the modification is technical data for the development of the new item.</p> <p>(2) Information enumerated on the USML (<i>i.e.</i>, not controlled pursuant to a catch-all USML paragraph);</p> <p>(3) Classified information for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article or a 600 series item subject to the EAR;</p> <p>(4) Information covered by an invention secrecy order; or</p>
--	---

<p>(5) Information, such as decryption keys, network access codes, or passwords that would allow access to other “technology” in clear text or “software”</p> <p>(b) “Technology” does not include:</p> <ul style="list-style-type: none">(1) Non-proprietary general system descriptions;(2) Information on basic function or purpose of an item; or(3) Telemetry data as defined in note 2 to Category 9, Product Group E (see Supplement No. 1 to Part 774 of the EAR).	<p>(5) Information, such as decryption keys, network access codes, or passwords that would allow access to other technical data in clear text or software (See §127.1(b)(4) of this subchapter).</p> <p>(b) Technical data does not include:</p> <ul style="list-style-type: none">(1) Non-proprietary general system descriptions;(2) Information on basic function or purpose of an item; or(3) Telemetry data as defined in note 3 to USML Category XV(f) (<i>see</i> §121.1 of this subchapter).
--	--

3. Published/Public Domain

§734.7 Published.

(a) Except as set forth in paragraph (b) of this section, unclassified “technology” or “software” is “published,” and is thus not “technology” or “software” subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:

- (1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;
- (2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;
- (3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;
- (4) Public dissemination (i.e., unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting on the Internet on sites available to the public; or
- (5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for

§120.11 Public Domain

(a) Except as set forth in paragraph (b), unclassified information and software are in the public domain, and are thus not technical data or software subject to the ITAR, when they have been made available to the public without restrictions upon their further dissemination such as through any of the following:

- (1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;
- (2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;
- (3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;
- (4) Public dissemination (i.e., unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting to the Internet on sites available to the public; or
- (5) Submission of a written composition, manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for

<p>publication or presentation.</p> <p>(b) Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in §740.13(e) of the EAR.</p>	<p>publication or presentation.</p> <p>(b) Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without an authorization from</p> <ol style="list-style-type: none"> (1) the Directorate of Defense Trade Controls; (2) the Department of Defense’s Office of Security Review; (3) the relevant U.S. government contracting entity with authority to allow the technical data or software to be made available to the public; or (4) Another U.S. government official with authority to allow the technical data or software to be made available to the public. <p><i>Note 1:</i> Section 127.1(a)(6) prohibits, without written authorization from the Directorate of Defense Trade Controls, U.S. and foreign persons from exporting, reexporting, retransferring, or otherwise making available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in paragraph (b) of this section.</p> <p><i>Note 2:</i> An export, reexport, or retransfer of technical data or software that was made publically available by another person without authorization is not a violation of this subchapter, except as described in §127.1(a)(6).</p>
--	---

4. Arises During, or Result from, Fundamental Research

§734.8 “Technology” that Arises During, or Results from, Fundamental Research.

(a) “Technology” that arises during, or results from, fundamental research and is ‘intended to be published’ is thus not “subject to the EAR.”

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technology that arises during or results from fundamental research” except to the extent that such inputs are “technology” that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution or company may decide to restrict or protect the release or publication of “technology” contained in research results. Once a decision is made to maintain such “technology” as restricted or proprietary, the “technology,” if within the scope of § 734.3(a), becomes “subject to the EAR.”

(b) *Prepublication review.* “Technology” that arises during, or results, from fundamental research is “intended to be published” to the extent that the researchers are free to publish the

§120.49 Technical data that Arises During, or Results from, Fundamental Research

(a) *Technical Data arising during, or resulting from, fundamental research.* Unclassified information that arises during, or results from, fundamental research and is intended to be published is not technical data when the research is:

- (1) Conducted in the United States at an accredited institution of higher learning; or
- (2) Funded, in whole or in part, by the U.S. government.

Note 1 to paragraph (a): The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technical data that arises during or results from fundamental research” except to the extent that such inputs are technical data that arose during or resulted from earlier fundamental research.

Note 2 to paragraph (a): There are instances in the conduct of research, whether fundamental, basic, or applied, where a researcher, institution or company may decide to restrict or protect the release or publication of technical data contained in research results. Once a decision is made to maintain such technical data as restricted or proprietary, the technical data becomes subject to the ITAR.

(b) *Prepublication review.* Technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data

technology contained in the research without restriction or delay. “Technology” that arises during or results from fundamental research subject to prepublication review is still “intended to be published” when:

(1) Prepublication review is conducted solely to ensure that publication would not compromise patent rights, so long as the review causes no more than a temporary delay in publication of the research results;

(2) Prepublication review is conducted by a sponsor of research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers; or

(3) With respect to research conducted by scientists or engineers working for a Federal agency or a Federally Funded Research and Development Center (FFRDC), within any appropriate system devised by the agency or the FFRDC to control the release of information by such scientists and engineers.

Note 1 to paragraph (b): Although “technology” arising during or resulting from fundamental research is not considered “intended to be published” if researchers accept restrictions on its publication, such “technology” will nonetheless qualify as “technology” arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Except as provided in § 734.11,

contained in the research without any restriction or delay, including U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.

Note 1 to paragraph (b): Although technical data arising during or resulting from fundamental research is not considered “intended to be published” if researchers accept restrictions on its publication, such technical data will nonetheless qualify as technical data arising during or resulting from fundamental research once all such restrictions have expired or have been removed.

Note 2 to paragraph (b): Research that is voluntarily subjected to

“technology” that is subject to other publication restrictions, such as U.S. government-imposed access and dissemination controls, is not “intended to be published.”

(c) *Fundamental research definition.* “Fundamental research” means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) “Basic Research” means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) “Applied research” means the effort that:

- (i) Normally follows basic research, but may not be severable from the related basic research;
- (ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and
- (iii) Attempts to advance the state of the art.

U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls.

Note 3 to paragraph (b): Technical data resulting from U.S. government funded research that is subject to government-imposed access and dissemination or other specific national security controls qualifies as technical data resulting from fundamental research, provided that all government-imposed national security controls have been satisfied.

(c) *Fundamental research definition.* Fundamental research means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

(1) Basic Research means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

(2) Applied research means the effort that:

- (i) Normally follows basic research, but may not be severable from the related basic research;
- (ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and
- (iii) Attempts to advance the state of the art.

5. Educational Information

§734.9 [Reserved]	n/a
-------------------	-----

6. Patents

<p>§734.10 Patents. “Technology” is not “subject to the EAR” if it is contained in:</p> <p>(a) A patent or an open (published) patent application available from or at any patent office;</p> <p>(b) A published patent or patent application prepared wholly from foreign-origin technology where the application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office;</p> <p>(c) A patent application, or an amendment, modification, supplement or division of an application, and authorized for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office, 37 CFR part 5; or</p> <p>(d) A patent application when sent to a foreign country before or within six months after the filing of a United States patent application for the purpose of obtaining the signature of an inventor who was in the United States when the invention was made or who is a co-inventor with a person residing in the United States.</p>	N/A
---	-----

7. Development

N/A	<p>§120.47 Development</p> <p>Development is related to all stages prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. Development includes modification of the design of an existing item.</p>
-----	--

8. Production

N/A	<p>§120.48 Production</p> <p>Production means all production stages, such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance. This includes “serial production” where commodities have passed production readiness testing (i.e., an approved, standardized design ready for large scale production) and have been or are being produced on an assembly line for multiple commodities using the approved, standardized design.</p>
-----	--

9. Required & Peculiarly responsible (in the EAR)

§772.1 “Required”. (General Technology Note)—

As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such “required” “technology” or “software” may be shared by different products. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Note 1: The references to “characteristics” and “functions” are not limited to entries on the CCL that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, ECCN 9A610.a controls “military aircraft specially designed for a military use that are not enumerated in USML paragraph VIII(a).” No performance level is identified in the entry, but the control characteristic of the aircraft is that it is specially designed “for military use.” Thus, any technology, regardless of significance, peculiar to making an aircraft “for military use” as opposed to, for example, an aircraft controlled

§120.46 Required

(a) As applied to technical data, the term required refers to only that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such required technical data may be shared by different products.

Note 1: The references to “characteristics” and functions” are not limited to entries on the USML that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, USML Category VIII(a)(1) controls aircraft that are “bombers.” No performance level is identified in the entry, but the characteristic of the aircraft that is controlled is that it is a bomber. Thus, any technical data, regardless of significance, peculiar to making an aircraft a bomber as opposed to, for example, an aircraft controlled under ECCN 9A610.a or ECCN 9A991.a, would be technical data required for a bomber

<p><i>under ECCN 9A991.a, would be technical data “required” for an aircraft specially designed for military use thus controlled under ECCN 9E610.</i></p> <p><i>Note 2: The ITAR and the EAR often divide within each set of regulations or between each set of regulations (a) controls on parts, components, accessories, attachments, and software and (b) controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated. Moreover, with the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data or “technology” is the same as the jurisdictional status of the defense article or “item subject to the EAR” to which it is directly related. Thus, if technology is directly related to the production of a 9A610.x aircraft component that is to be integrated or installed in a USML VIII(a) aircraft, then the technology is controlled under ECCN 9E610, not USML VIII(i).</i></p> <p><i>772.1 Peculiarly responsible. An item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR unless:</i></p> <p>(1) The Department of Commerce has determined otherwise in a commodity classification determination;</p> <p>(2) Reserved;</p>	<p>and thus controlled under USML Category VIII(i).</p> <p><i>Note 2: The ITAR and the EAR often divide within each set of regulations or between each set of regulations (a) controls on parts, components, accessories, attachments, and software and (b) controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated. With the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data is the same as the jurisdictional status of the defense article or item “subject to the EAR” to which it is directly related. Thus, if technology is directly related to the production of an ECCN 9A610.x aircraft component that is to be integrated or installed in a USML Category VIII(a) aircraft, the technology is controlled under ECCN 9E610, not USML Category VIII(i).</i></p> <p><i>Note 3: Technical data is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless:</i></p> <p>1. The Department of State has determined otherwise in a commodity jurisdiction determination;</p> <p>2. Reserved;</p>
--	--

<p>(3) It is identical to information used in or with a commodity or software that:</p> <ul style="list-style-type: none"> (i) Is or was in production (<i>i.e.</i>, not in development); and (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons; <p>(4) It was or is being developed with “knowledge” that it would be for use in or with commodities or software (i) described in an ECCN <i>and</i> (ii) also commodities or software either not ‘enumerated’ on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;</p> <p>(5) It was or is being developed for use in or with general purpose commodities or software, <i>i.e.</i>, with no “knowledge” that it would be for use in or with a particular commodity or type of commodity; <i>or</i></p> <p>(6) It was or is being developed with “knowledge” that it would be for use in or with commodities or software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) exclusively for use in or with EAR99 commodities or software.</p>	<p>3. It is identical to information used in or with a commodity or software that:</p> <ul style="list-style-type: none"> (i) Is or was in production (<i>i.e.</i>, not in development); and (ii) Is not a defense article; <p>4. It was or is being developed with knowledge that it is or would be for use in or with both defense articles and commodities not on the U.S. Munitions List; or</p> <p>5. It was or is being developed for use in or with general purpose commodities or software (<i>i.e.</i>, with no knowledge that it would be for use in or with a particular commodity).</p>
--	---

10. Export

<p>§734.13 Export.</p> <p>(a) Except as set forth in § 734.17, “export” means:</p> <p>(1) An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;</p> <p>(2) Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”);</p> <p>(3) Transferring by a person in the United States of registration, control, or ownership of:</p> <p>(i) A spacecraft subject to the EAR that is not eligible for export under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country, or</p> <p>(ii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country; or</p> <p>(4) [Reserved]</p> <p>(5) [Reserved]</p>	<p>§120.17 Export</p> <p>(a) Except as set forth in §§ 120.52, 126.16, or 126.17 of this subchapter, export means:</p> <p>(1) An actual shipment or transmission out of the United States, including the sending or taking of a defense article outside of the United States in any manner;</p> <p>(2) Releasing or otherwise transferring technical data or software (source code or object code) to a foreign person in the United States (a “deemed export”);</p> <p>(3) Transferring by a person in the United States of registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite subject to the ITAR;</p> <p>(4) Releasing or otherwise transferring a defense article to an embassy or to any agency or subdivision of a foreign government, such as a diplomatic mission, in the United States;</p> <p>(5) Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or</p>
--	---

<p>(6) Releasing or otherwise transferring decryption keys, network access codes, passwords, “software,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “software” to a foreign national.</p> <p>(b) Any release in the United States of “technology” or “source code” to a foreign national is a deemed export to the foreign national’s most recent country of citizenship or permanent residency.</p> <p>(c) The export of an item that will transit through a country or countries or will be transshipped in a country or countries to a new country, or are intended for reexport to the new country, is deemed to be an export to the new country.</p>	<p>abroad;</p> <p>(6) Releasing or otherwise transferring information such as decryption keys, network access codes, passwords, or software, providing or physical access that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred; or</p> <p>(7) Making technical data available via a publicly available network (e.g., the Internet).</p> <p>(b) Any release in the United States of technical data or software to a foreign person is a deemed export to all countries in which the foreign person has held citizenship or permanent residency.</p>
---	--

11. Reexport

<p>§734.14 Reexport. (a) Except as set forth in §§ 734.18 and 734.20, “reexport” means:</p> <p>(1) An actual shipment or transmission of an item from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;</p> <p>(2) Releasing or otherwise transferring “technology” or “source code” to a foreign national of a country other than the foreign country where the release or transfer takes place (a “deemed reexport”);</p> <p>(3) Transferring by a person outside the United States of registration, control, or ownership of:</p> <p>(i) A spacecraft subject to the EAR that is not eligible for reexport under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country, or</p> <p>(ii) Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country; or</p> <p>(4) Releasing or otherwise transferring outside of the United States decryption keys, network access codes, passwords,</p>	<p>§120.19 Reexport (a) Except as set forth in section 120.52 of this subchapter, reexport means:</p> <p>(1) An actual shipment or transmission of a defense article from one foreign country to another foreign country, including the sending or taking of a defense article to or from such countries in any manner;</p> <p>(2) Releasing or otherwise transferring technical data or software to a foreign person of a country other than the foreign country where the release or transfer takes place (a “deemed reexport”);</p> <p>(3) Transferring by a person outside of the United States of registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR to a foreign person outside the United States; or</p> <p>(4) Releasing or otherwise transferring outside of the United States information, such as decryption keys, network access</p>
---	--

<p>“software,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “software” to a foreign national.</p> <p>(b) Any release outside of the United States of “technology” or “source code” subject to the EAR to a foreign national of another country is a deemed reexport to the foreign national’s most recent country of citizenship or permanent residency, except as described in § 734.20.</p> <p>(c) The reexport of an item subject to the EAR that will transit through a country or countries or will be transshipped in a country or countries to a new country, or are intended for reexport to the new country, is deemed to be a reexport to the new country.</p>	<p>codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred.</p> <p>(b)[Reserved]</p>
--	---

12. Release

<p>§734.15 Release.</p> <p>(a) Except as set forth in § 734.18, “technology” and “software” are “released” through:</p> <p>(1) Visual or other inspection by a foreign national of items that reveals “technology” or “source code” subject to the EAR to a foreign national;</p> <p>(2) Oral or written exchanges with a foreign national of “technology” in the United States or abroad; or</p> <p>(3) The application by U.S. persons of “technology” or “software” to situations abroad using personal knowledge or technical experience acquired in the United States, to the extent that the application reveals to a foreign national “technology” or “source code” subject to the EAR.</p> <p>(b) Reserved</p>	<p>§120.50 Release</p> <p>(a) Except as set forth in section §120.52 of this subchapter, technical data and software are released through:</p> <p>(1) Visual or other inspection by foreign persons of a defense article that reveals technical data or software to a foreign person; or</p> <p>(2) Oral or written exchanges with foreign persons of technical data in the United States or abroad.</p> <p>(b) Reserved</p>
---	---

13. Retransfer and Transfer (In-Country)

<p>§734.16 Transfer (in-country).</p> <p>Except as set forth in § 734.18, a transfer (in-country) is a change in end use or end user of an item within the same foreign country. “Transfer (in-country)” is synonymous with “in-country transfer.”</p>	<p>§120.51 Retransfer</p> <p>Except as set forth in section 120.52 of this subchapter, a retransfer is a change in end use or end user of a defense article within the same foreign country.</p>
---	---

14. Activities that are Not Exports, Reexports, Releases, Retransfers, or Transfers

<p>§734.18 Activities that are not exports, reexports, or transfers</p> <p>(a) The following activities are not exports, reexports, or transfers:</p> <p>(1) Launching a spacecraft, launch vehicle, payload, or other item into space.</p> <p>(2) While in the United States, releasing “technology” or “software” to United States citizens, persons lawfully admitted for permanent residence in the United States, or persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).</p> <p>(3) Shipping, moving, or transferring items between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, or the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census.</p> <p>(4) Sending, taking, or storing “technology” or “software” that is:</p> <p>(i) Unclassified;</p> <p>(ii) Secured using ‘end-to-end encryption;’</p>	<p>§120.52 Activities that are Not Exports, Reexports, or Retransfers</p> <p>(a) The following activities are not exports, reexports, or retransfers:</p> <p>(1) Launching a spacecraft, launch vehicle, payload, or other item into space;</p> <p>(2) While in the United States, releasing technical data or software to a U.S. person;</p> <p>(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; and</p> <p>(4) Sending, taking, or storing technical data or software that is:</p> <p>(i) Unclassified;</p> <p>(ii) Secured using end-to-end encryption;</p>
--	---

<p>(iii) Secured using cryptographic modules (hardware or “software”) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and</p> <p>(iv) Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation.</p> <p>(b) <i>Definitions.</i> For purposes of this section, ‘end-to-end encryption’ means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.</p> <p>(c) The ability to access “technology” or “software” in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such “technology” or “software.”</p> <p><i>Note to § 734.18: Releasing “technology” or “software” to any person with knowledge that a violation will occur is prohibited by §736.2(b)(10) of the EAR.</i></p>	<p>(iii) Secured using cryptographic modules (hardware or software) as compliant with the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and</p> <p>(iv) Not stored in a country proscribed in §126.1 of this subchapter or the Russian Federation.</p> <p>(b) For purposes of this section, end-to-end encryption means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.</p> <p>(c) The ability to access technical data or software in encrypted form does not constitute the release or export of such technical data or software.</p> <p><i>Note:</i> See §127.1 of this subchapter for prohibitions on the release or transfer of technical data or software, in any form, to any person with knowledge that a violation will occur.</p>
---	--

15. Scope of a License

<p>§750.7 Issuance of Licenses</p> <p>(a) Scope. Unless limited by a condition set out in a license, the export, reexport, or transfer (in-country) authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. The applicant must inform the other parties identified on the license, such as the ultimate consignees and end users, of the license's scope and of the specific conditions applicable to them. BIS grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted. A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity's foreign nationals who are permanent and regular employees (and who are not proscribed persons under U.S. law) of the entity's facility or facilities authorized on the license, except to the extent a license condition limits or prohibits the release of the technology to nationals of specific countries or country groups.</p>	<p>§123.28 Scope of License</p> <p>Unless limited by a condition set out in a license, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. DDTC grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted.</p> <p>§124.1(e)</p> <p>Unless limited by a condition set out in an agreement, the export, reexport, retransfer, or temporary import authorized by a license is for the item(s), end-use(s), and parties described in the agreement, license and any letters of explanation. DDTC approves agreements and grants licenses in reliance on representations the applicant made in or submitted in connection with the agreement, letters of explanation, and other documents submitted.</p>
--	--

16. Export of Controlled Information to US Persons Abroad

<p>§740.9(a)(3) “Technology,” regardless of media or format, may be exported by or to a U.S. person or a foreign national employee of a U.S. person, traveling or on temporary assignment abroad subject to the following restrictions subject to the following restrictions:</p> <p>(i) Foreign nationals may only export or receive such “technology” as they are authorized to receive through a license, license exception other than TMP or because no license is required.</p> <p>(ii) “Technology” exported under this authorization may only be possessed or used by a U.S. person or authorized foreign national and sufficient security precautions must be taken to prevent the unauthorized release of the “technology.” Such security precautions include encryption of the “technology,” the use of secure network connections, such as Virtual Private Networks, the use of passwords or other access restrictions on the electronic device or media on which the “technology” is stored, and the use of firewalls and other network security measures to prevent unauthorized access.</p> <p>(iii) The U.S. person is an employee of the U.S. government or is directly employed by a U.S. person and not, e.g., by a foreign subsidiary.</p> <p>(iv) “Technology” authorized under this exception may not be used for foreign production purposes or for technical assistance unless authorized through a license or license exception other than</p>	<p>§125.4(b)(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or a foreign person employee of a U.S. person, travelling or on temporary assignment abroad subject to the following restrictions:</p> <p>(i) Foreign persons may only export or receive such technical data as they are authorized to receive through a separate license or other approval.</p> <p>(ii) The technical data exported under this authorization is to be possessed or used solely by a U.S. person or authorized foreign person and sufficient security precautions must be taken to prevent the unauthorized release of the technology. Such security precautions may include encryption of the technical data, the use of secure network connections, such as virtual private networks, the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored, and the use of firewalls and other network security measures to prevent unauthorized access.</p> <p>(iii) The U.S. person is an employee of the U.S. government or is directly employed by a U.S. person and not by a foreign subsidiary.</p> <p>(iv) Technical data authorized under this exception may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.</p>
---	--

<p>TMP.</p> <p>(v) The U.S. person employer of foreign nationals must document the use of this exception by foreign national employees, including the reason that the “technology” is needed by the foreign nationals for their temporary business activities abroad on behalf of the U.S. person.</p>	<p>(v) The U.S. employer of foreign persons must document the use of this exemption by foreign person employees, including the reason that the technical data is needed by the foreign person for their temporary business activities abroad on behalf of the U.S. person.</p> <p>(vi) Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed).</p>
--	--

17. Release of Protected Information

<p>§764.2(l)</p> <p>No person may “release” or otherwise transfer information, such as decryption keys, network access codes, or passwords, that would allow access to other “technology” in clear text or “software” with “knowledge” that the release will result, directly or indirectly, in an unauthorized export, reexport, or transfer of the “technology” in clear text or “software.” Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled “technology” or “software.”</p>	<p>§127.1(b)(4)</p> <p>To release or transfer information, such as decryption keys, network access codes, or passwords that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software.</p>
---	--

18. New Section 127.1(a)(6) prohibition

<p>N/A</p>	<p>§127.1(a)(6)</p> <p>(6) To export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in section 120.11(b) of this subchapter.</p>
-------------------	--



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0003

Tracking Number: 1jz-8jb9-tztb

Document Information

Date Posted:
Jul 27, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Anonymous Kennedy

Comment

I believe this is a blatant attempt to circumvent my Constitutional rights under the First and Second Amendments. Online forums are a public place as many do not require membership.

This will harm gunsmiths, manufacturers, reloaders, and do-it-yourselfers who all require the ability to distribute or obtain the information they rely on to conduct their businesses.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0004

Tracking Number: 1jz-8jcb-7r2a

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

John DeLallo

Comment

Regarding:

International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

- Document Contents : ...State proposes to amend the International Traffic in Arms [[Page 31526]] Regulations (ITAR) to update the definitions of ``defense article,`` ``defense services,`` ``technical data,`` ``public...

Proposed Rule by DOS on 06/03/2015 ID:
DOS_FRDOC_0001-3265

This proposal is a blatant attack on the Bill of Rights, and if adopted will negate the First Amendment, the Second Amendment, and serve as a non judicial imposition of absurd gun control on a Free Nation. This proposal must never be allowed. It will, in fact, create a new class of criminals, consisting of publishers, lawful firearm owners, and manufacturers and advertisers. The courtesy of a reply is requested.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: BIS-2015-0019-0005

Tracking Number: 1jz-8jcg-dojk

Comment

Document Information

This rulemaking also proposes amendments to the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software.

Date Posted:
Jul 27, 2015

RIN:
0694-AG32

[Show More Details](#)

-- The ability to stop online publishing of anything that could possibly be related to ITAR?

Submitter Information

"ITAR regulations dictate that information and material pertaining to defense and military related technologies (items listed on the U.S. Munitions List) may only be shared with U.S. Persons unless authorization from the Department of State is received or a special exemption is used.[3] U.S. Persons (including organizations) can face heavy fines if they have, without authorization or the use of an exemption, provided foreign persons with access to ITAR-protected defense articles, services or technical data" - wikipedia

Submitter Name:
David Hendrickson

So if I transmit a breakdown of say an AR-15 which is under the USML is under one of 20 categories (Firearms, Close Assault Weapons and Combat Shotguns) to a NON US person I will have the weight of the government fall upon me.

If I were to send a diagram of a helmet (Personal protective equipment) I am also in violation.

If I was a military historian I am in violation for providing specs on military vehicles and ships. (Vessels of War and Special Naval Equipment Tanks and Military Vehicles)

I can't transmit anything dealing with (Spacecraft Systems and Associated Equipment) when talking to a European Space Agency technician because they are a non US person.

What you are trying to do with this 1 sentence is to make

thousands of people "enemies of the state".
You trying to backdoor the United States Constitution.
This sentence needs to be removed from the final draft.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0006

Tracking Number: 1jz-8jch-be5a

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Anonymous Anonymous

Comment

Regarding:

International Traffic in Arms: Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

- Document Contents : ...State proposes to amend the International Traffic in Arms [[Page 31526]] Regulations (ITAR) to update the definitions of ``defense article,`` ``defense services,`` ``technical data,`` ``public...

Proposed Rule by DOS on 06/03/2015 ID:
DOS_FRDOC_0001-3265

This proposal is a blatant attack on the Bill of Rights, and if adopted will negate the First Amendment, the Second Amendment, and serve as a non judicial imposition of absurd gun control on a Free Nation. This proposal must never be allowed. It will, in fact, create a new class of criminals, consisting of publishers, lawful firearm owners, and manufacturers and advertisers. The courtesy of a reply is requested.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0007

Tracking Number: 1jz-8jco-vtgs

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:

John Biltz

Comment

I realize that the present administration does not have the least bit of respect for the constitution but surely they must realize what an act of rape this would be for at least 2 amendments of the Bill of Rights. But of course they realize this and it is why they are trying to slip this in behind everyone's back in such an underhanded and despicable manner.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0008

Tracking Number: 1jz-8jcu-w57g

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

mark Anonymous

Comment

I find it sickening how widespread this reaches. The US Munitions list is rather large and lists everything from Bombers to simple weapons owned privately by millions of Americans. Asking private individuals to request permission from the state department in order to move a privately owned rifle is waste of both time and tax payer funds. Also this mentions technical data, which easily would include information on designs and manufacturing processes for guns and ammunition and by transferring this information everyone from private gunsmiths to US Citizen who assemble there own registered firearms from parts would be in violation of these proposed rules.

I am not sure if common sense has escaped the creator of this regulation, but excluding all items with a purchase price under a set dollar amount would rectify this issue (ie.. any item with a sale price of \$7,500.00 or higher) This way private gun owners and collectors can continue freedoms provided under the 2nd amendment and a items which absolutely need to be protected (missiles, Rockets, and other weapons of war).



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0009

Tracking Number: 1jz-8jee-shqk

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Concerned American

Comment

To whom it may concern:

I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State Department a wide-ranging power to monitor and control gun-related speech on the Internet.

The new language – which includes making technical data available via a publicly available network (e.g., the Internet) – could put anyone who violates this provision in danger of facing decades in prison and massive fines.

So posting information on virtually any firearm or ammunition could be defined by the Obama administration as requiring, not only government permission, but potentially a government license. This means violators would potentially face significant criminal penalties.

I also oppose the addition of the word software into these regulations, as it appears to be a not-so-veiled effort to ban 3-D printers.

I urge you to repeal these new regulations in their entirety. Whether you like it or not, the First and Second Amendments are still the law of the land!

Sincerely,

Concerned American



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0010

Tracking Number: 1jz-8jg4-gps3

Document Information

Date Posted:
Jul 27, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Edward Kosewicz

Comment

I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State Department a wide-ranging power to monitor and control gun-related speech on the Internet.

The new language -- which includes making technical data available via a publicly available network (e.g., the Internet) -- could put anyone who violates this provision in danger of facing decades in prison and massive fines.

So posting information on virtually any firearm or ammunition could be defined by the Obama administration as requiring, not only government permission, but potentially a government license. This means violators would potentially face significant criminal penalties.

I also oppose the addition of the word software into these regulations, as it appears to be a not-so-veiled effort to ban 3-D printers.

I urge you to repeal these new regulations in their entirety. Whether you like it or not, the First and Second Amendments are still the law of the land!

Sincerely,



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0011

Tracking Number: 1jz-8jiz-gwtr

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Neil Sagers

Comment

I am very concerned about the State Department's proposed changes to regulate internet posts concerning firearms or related technology under ITAR regulations posted Jun 3, 2015 as RIN 0694-AG32. This proposal would regulate public or private communications by individuals over undefined firearms technology. This prior restraint on free speech runs contrary to the American idea of freedom and the First Amendment. How is a person to know if something they have done as a hobby constitutes "regulated speech" until they are arrested and charged with penalties that include years in prison and huge fines?

Strict scrutiny is required of any law or regulation that limits free speech in that the government must show a compelling interest in regulating the speech and that the regulations are the least obtrusive method of obtaining the desired goal. The proposed regulation implements a prior restraint on undefined speech and there can be no strict scrutiny of something undefined.

This proposed rulemaking will have, at a minimum, a chilling effect on the free and open exchange of ideas on firearms. What these regulations would do is to define export to include potentially any gun-related communication on the Internet or social media. This crosses a broad spectrum of concerns from websites talking about things such as reloading, firearms modifications, designs or even maintenance issues to virtually any technical data. In fact, these regulations are so broad that it could potentially include virtually any gun-related communication of a functional how to nature. I urge you to protect everyone's First and Second Amendment rights by rejecting this ill-considered the proposed regulation.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0012

Tracking Number: 1jz-8jxy-makk

Document Information

Date Posted:

Jul 27, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Keith Black

Comment

By "codifying current law" the administration will use the State Department to classify any communication about firearms as an "export" subject to ITAR regulations. The Second Amendment would be subject to the whims of the State Department.

This means the creation of any public or private letter, newsletter, brochure, email, web posting, social media contribution, etc. discussing anything from reloading, firearms design and/or modification, repair and/or maintenance, training, or any technical/specification data could land someone in jail for years! Furthermore, anyone without a "green card" might not even be allowed to know any of this information. That means the most rabid of bureaucrats would most certainly create a new regulatory crime if someone working here without a "green card" were to take a self-defense firearms course. And, yes, both the teacher and the student would be criminals in the government's eyes. Do you see where this is going? Guns today. Medicine and health tomorrow. Money and finance next week. The Internet and smart phones next month. All human communications next year.

This regulatory change is extremely dangerous because any administration could twist it to meet its agenda.



Office of the Vice Provost for Research

July 31, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

The University of Pennsylvania (Penn) supports the open exchange of information in fulfillment of our mission of research, education, and service. As a result, Penn does not accept restrictions on access, publication, dissemination, or participation in research and classroom activities based on national origin.

Penn welcomes the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32: Revisions to Definitions in the Export Administration Regulations. We appreciate the effort involved in harmonizing and streamlining these definitions and view most of the changes as positive. For example, the exclusion of sending, taking, or storing software secured using end-to-end encryption from export activities is welcome to the academic research community, as it will reduce faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. We also appreciate the BIS confirmation in this proposed rule of our understanding of “fundamental research” at universities, and in particular the clear statement that short pre-publication review of the results of fundamental research by sponsors to ensure that publication does not compromise patent rights (§734.8(b)(1)) or to insure that the publication does not inadvertently divulge sponsor provided proprietary information (§734.8(b)(2)) does not make the research subject to the Export Administration Regulations (EAR).

We offer the following comments and suggestions.

Changes to Educational Information

Under the current EAR (§734.3(b)(3)(iii) and §734.9), “educational information” is defined as information “released by instruction in catalog courses and associated teaching laboratories of academic institutions,” and excludes such information from the

scope of the EAR. The proposed rule removes § 734.9 and this definition, and replaces it in proposed EAR §734.3(b)(3)(iii) with information and software that “concern general scientific, mathematical, or engineering principles commonly taught in schools *and* released by instruction in a catalog course or associated teaching laboratory at an academic institution” (emphasis added). We believe that this change narrows the definition of educational information excluded from the EAR, even though the comments to the proposed final rule state: “This proposed rule is not intended to change the scope of the current §734.9” [80 FR 31507, June 3, 2015]. Universities continually modify and create new and novel course content based on evolving technologies, some of which include design laboratories. Under the proposed change, it is not clear that novel course content would be considered *commonly taught* or if it might contain more than *general principles* and therefore be subject to the EAR.

At Penn, enrollment in courses is open to anyone, regardless of citizenship or national origin, who has completed any educational prerequisites. A narrow interpretation of the proposed revised EAR §734.3(b)(3)(iii) would inhibit the ability of U.S. universities to develop new courses in emerging areas of science and engineering that are critical to the future competitiveness of the industrial sector.

Penn recommends removing the phrase “concern general scientific, mathematical, or engineering principles commonly taught in schools” and that the current “released by instruction in catalog courses and associated teaching laboratories of academic institutions” be retained for proposed EAR §734.3(b)(3)(iii). Alternatively, we endorse the recommendation by the Council on Government Relations (COGR) and the Association of American Universities (AAU) to change the “and” in the proposed definition to an “or”, to avoid unintentionally limiting this definition (*i.e.*, to clearly cover a new university course in an emerging technology area so long as it is included in a course catalog), and to achieve the government’s stated goal as set forth in the Federal Register of not changing the scope of the current EAR §734.9.

“Fundamental research,” “technology,” and “software”

Currently, publicly available technology and software arising during, or resulting from, fundamental research are not subject to the EAR (§734.3(b)(3)). Under the proposed EAR §734.8(a), “technology,” but not software, that arises during, or results from, fundamental research and is intended to be published, is not subject to the EAR. This is a significant change that will complicate and restrict university research. Both “software” and “technology” resulting from university research are published. Under the proposed change, a natural-language document written by a researcher could be “technology” arising during fundamental research while a computer-language document could be subject to deemed export restrictions, even though it arises during fundamental research and is intended to be published. We suggest that the language be revised to distinguish between source code, which may be published as the result of fundamental research, and other software. As an alternative, Penn also endorses and would support the recommendation in the comments from COGR and AAU on this issue.

Effective Date of the Final Rule

RIN 0694-AG32 (and the corresponding RIN 1400-AD70 to revise the ITAR regulations) could have a significant and negative impact on regulatory burden for Penn, if the final rules are adopted as published and without the changes suggested by COGR and AAU.

The proposed changes to the ITAR §120.49(b) Prepublication Review would significantly increase Penn's administrative burden, as described in our comment to DDTC (attached). If the proposed rule is adopted as written and without changes, Penn would have a very difficult time achieving compliance within 30 days after the publication date of the final rule. We suggest, at a minimum, that the effective date be six months after publication of the final rule.

Other Comments

Penn works closely with the Council on Governmental Relations (COGR), the Association of American Universities (AAU), and the Association of University Export Control Officers (AUECO) and has reviewed their comments being submitted concerning the proposed EAR and ITAR changes. Where no Penn comment is offered, we concur with the comments offered by COGR, AAU, and AUECO.

Penn appreciates the opportunity to provide comments on these proposed changes.

Sincerely,



Dawn A. Bonnell, PhD
Vice Provost for Research
Henry Robinson Towne Professor of Engineering and Applied Science
Materials Science and Engineering

Attachments



Office of the Vice Provost for Research

July 31, 2015

C. Edward Peartree
Director
Office of Defense Trade Controls Policy
U.S. Department of State
2401 E Street, N.W.
Attn.: ITAR Amendment
Washington, DC 20522

RE: ITAR Amendment – Revisions to Definitions; Data Transmission and Storage
(RIN 1400-AD70)

Dear Mr. Peartree:

The University of Pennsylvania (Penn) supports the open exchange of information in fulfillment of our mission of research, education, and service. As a result, Penn does not accept restrictions on access, publication, dissemination, or participation in research and classroom activities based on national origin.

Penn welcomes the opportunity to comment in response to the Directorate of Defense Trade Controls (DDTC) RIN 1400-AD70: International Traffic in Arms; Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions.

We recognize and appreciate the efforts of the Departments of Commerce, Defense, and State to reform U.S. export controls and view most of the proposed changes as positive. For example, the exclusion of sending, taking, or storing software secured using end-to-end encryption from export activities is welcome to the academic research community, as it will reduce faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. RIN 1400-AD70 and the accompanying RIN 0694-AG32 regarding revisions to EAR definitions, include many positive proposed changes, advance harmonization goals, and in many areas would reduce regulatory burdens on universities.

However, as written, several proposed changes would result in significant increased and new administrative burdens in the management of industry-sponsored research at Penn.

We offer the following comments:

Fundamental Research and Prepublication Review

Penn favors defining “fundamental research” separately from the definition of “public domain”. Penn also supports that the proposed ITAR regulation defines that information arising during, or resulting from, fundamental research that is intended to be published is not technical data subject to the ITAR. However, the addition of proposed ITAR §120.49(b) on prepublication review is highly problematic. Proposed ITAR §120.49(b) states that “technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data contained in the research without any restriction or delay, including ... research sponsor proprietary information review.” Penn considers this to be at odds with NSDD-189, which distinguishes fundamental research, the results of which are published and shared broadly within the scientific community, from proprietary and restricted research, the results of which are restricted for proprietary or national security reasons. We believe that NSDD-189 does not contemplate that a brief, temporary period for a commercial sponsor to conduct a “proprietary information review” should be treated as a *restriction* or *delay* on publication, and, thus, bring the research outside the definition of “fundamental research.”

While Penn does not accept dissemination controls on information arising from research, industry sponsors of university fundamental research generally require pre-review of publications, simply to ensure that no proprietary material inadvertently has made its way into the research report, and to give a company a brief opportunity to decide whether the research has resulted in any patentable inventions and to move expeditiously to file a patent application. Penn generally will agree to brief, time-limited reviews, often about 30 days. This is entirely different from accepting a publication restriction in which the sponsor must give *approval* before the researcher is able to publish. The current EAR §734.8 recognizes these distinctions. For example, current EAR § 734.8(b)(2) states: “Prepublication review by a sponsor of university research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research”; and current EAR §734.8(b)(3) states: “Prepublication review by a sponsor of university research solely to ensure that publication would not compromise patent rights does not change the status of fundamental research, so long as the review causes no more than a temporary delay in publication of the research results.” Neither case requires sponsor approval before the research is published or gives the sponsor the right to prevent the research from being published. The government has not explained why this principle, which has worked extremely well to advance university-industry research in areas governed by the EAR, should be any different in areas governed under ITAR.

In fiscal year 2015, Penn entered into more than 450 research agreements with industry sponsors. Currently, research under such agreements that include temporary and short-term publication reviews, without any affirmative approval requirement, is defined as fundamental research, regardless of whether the subject matter would otherwise fall under the ITAR or the EAR. The proposed ITAR exclusion from “fundamental research” if there is any brief pre-publication delay, will require not only hours of review of contract language, but also appropriate classification of technology and technical data prior to the start of the research activity on campus. This will result in significant delays, including increasing the time spent negotiating sponsored research agreements with commercial sponsors, obtaining commodity jurisdiction determinations in cases of classification uncertainty, implementing technology control plans, and applying for and obtaining licenses to enable participation of foreign nationals in the research, monitoring of those plans, and eventual removal of the plans once the sponsor review is complete. In our globally diverse research university community, the proposed change will result in increased regulatory burden on our faculty and support staff, increased numbers of license applications and licenses required, increased administrative expense (reducing the overall funding from the sponsor that is available to pay for direct research), and threats to our open, nondiscriminatory research environment.

Penn estimates that this requirement could result in the need for additional employees to support our export compliance infrastructure and will significantly increase administrative burden to faculty. We believe that there is no benefit to national security that accompanies this additional burden, and the publication in the Federal Register does not articulate any national security benefit outweighing these burdens, or why the ITAR approach differs from the EAR approach. Penn strongly recommends that language in proposed ITAR §120.49(b) be changed to match the language in the current EAR §734.8(b), so that the ITAR definitions of fundamental research and intent to publish conform with the university community’s understanding of the concept of fundamental research based in NSDD-189.

Effective Date of the Final Rule

Given the significant increase in administrative burden outlined above, if the proposed changes are finalized as currently written, Penn would have a very difficult time achieving compliance within 30 days after the publication date of the final rule, for all of our industry sponsored research. We suggest, at a minimum, that the effective date be six months after publication of the final rule. Penn also suggests that the final rule be applicable to new sponsored research contracts first entered into after the effective date that is chosen, and not have any retroactive effect regarding research that has already commenced as of the effective date, or a funding contract already entered into prior to the effective date.

Penn is a member of the Council on Governmental Relations (COGR) and the Association of American Universities (AAU), among other organizations. We have had the opportunity to review their comments being submitted concerning the proposed

ITAR and EAR changes. We concur with the comments submitted by these organizations.

Sincerely,

A handwritten signature in black ink that reads "Dawn A. Bonnell". The signature is written in a cursive, flowing style.

Dawn A. Bonnell, PhD
Vice Provost for Research
Henry Robinson Towne Professor of Engineering and Applied Science
Materials Science and Engineering



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0014

Tracking Number: 1jz-8k93-4wru

Document Information

Date Posted:

Aug 4, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Anonymous Anonymous

Comment

Regarding the definition of reexport in proposed 734.14:

734.14(a)(1): Using the unqualified phrase an item would make this definition overbroad and encompass items that are not subject to the EAR. Suggest inserting subject to the EAR immediately after an item in both places, so subparagraph (a)(1) would read: (1) An actual shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item subject to the EAR to or from such countries in any manner;

734.14(a)(2): Likewise, by not limiting technology and source code in proposed 734.14(a)(2), the proposed definition would encompass technology and source code that are not subject to the EAR. Suggest inserting subject to the EAR immediately after technology and source code, so paragraph (a)(2) would read: (2) Releasing or otherwise transferring technology or source code subject to the EAR to a foreign national of a country other than the foreign country where the release or transfer takes place (a deemed reexport);

734.14(a)(4): Finally, by not limiting the decryption keys, network access codes, passwords, software, or other information in proposed 734.14(a)(4), the proposed definition would encompass such items that are not subject to the EAR. Suggesting inserting subject to the EAR immediately after other information, so paragraph (a)(4) would read: (4) Releasing or otherwise transferring outside of the United States decryption keys, network access codes, passwords, software, or other information subject to the EAR with knowledge that such provision will cause or permit the transfer of other technology in clear text or software to a foreign national.

Regarding the scope of the EAR in proposed 734.18:

734.18(a)(4): Suggest inserting subject to the EAR immediately after technology or software, so paragraph (a)(4) would read: (4) Sending, taking, or storing technology or

software subject to the EAR that is:

Regarding proposed changes to 740.9:

740.9(a)(3)(iii): Suggest inserting or foreign national immediately after U.S. person, so subparagraph (a)(iii) would read: (iii) The U.S. person or foreign national is an employee of the U.S. Government or is directly employed by a U.S. person and not, e.g., by a foreign subsidiary.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0015

Tracking Number: 1jz-8k9w-8gqc

Document Information

Date Posted:

Aug 4, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Anonymous Anonymous

Comment

If this is the article about our President bypassing congress again with an executive order to interfere with my right to buy a gun and protect myself from being injured , then I cant wait until Donald is elected to repeal that executive order and keep the first and second amendments as they are now. Please just make laws that pertain to everyone including

Congressmen and Senators who think they are above the law and let each state handle its own affairs. No Obama Care

for instance. No bowing to anyone. No Czars. No releasing people who threaten our safety. No nuclear weapons for the middle east. No saying one thing to get elected and not doing what you promised. I'am sick of our government. I wish I

had my time back for protecting what i thought was a great country..now this country stinks.. I hope God is coming back just to punish our governments 500 or so idiots.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

For related information, [Open Docket Folder](#)

Comment

Utah State University supports the efforts being made to harmonize export control regulations contained in the Export Administration Regulations and in the International Traffic in Arms Regulations.

We endorse the comments you will be receiving from COGR and AAU, as they have been outlined to the memberships of those organizations. We are submitting a comment regarding the language at 120.49(b) Prepublication review, which states: "Technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data contained in the research without any restriction or delay..."

It has been common practice to allow sponsors the opportunity to review materials in preparation for publication to verify that sponsor proprietary information is not inadvertently included in a subsequent release of the material. Removing the institution's ability to treat such information as fundamental research introduces a level of uncertainty that will be extremely disruptive to institutions of higher education. A particular problem will be the impact on student involvement, where the project is the topic of a student's thesis or dissertation. While we see that note 1 to the paragraph provides that qualification of the data as having resulted from fundamental research may be restored after the restriction/delay has been removed, this approach will unavoidably dampen a professor/student dyad's likelihood of engaging in projects that exist under this cloud.

Additionally this could highly limit how we work with partnering industry and even our own, whole owned 501C3. We are dependent upon a the fundamental research exemption to help open up partnering possibilities. Any restrictions in this matter will specifically become more limiting in how we are able to work with associated

ID: BIS-2015-0019-0016

Tracking Number: 1jz-8kak-mrru

Document Information

Date Posted:

Aug 4, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Mark McLellan

companies.

The sense of this section, and of the agency's commentary on it, indicates that the intent has been to provide greater flexibility and make the environment more attractive for those that can contribute new knowledge through fundamental research. We ask that the definition be modified to reflect the parallel language in the EAR, which does not create this same barrier to collaboration between higher education and industry.

We appreciate the opportunity to comment on the proposed definitions and the efforts that have been made to reduce administrative burdens on the research community.

Mark R. McLellan, PhD | Vice President for Research &
Dean of the School of Graduate Studies
Utah State University | 1450 Old Main Hill | Logan, UT
84322-1450
PH (435) 797-1180 | FAX (435) 797-1367 | E-mail:
mark.mclellan@usu.edu



University of Pittsburgh

Office of Export Control Services

University Club B21
123 University Place
Pittsburgh, PA 15213
412-624-7400
Fax: 412-624-7409

July 31, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32)

Dear Ms. Hess:

Founded in 1787, the University of Pittsburgh – Of the Commonwealth of Higher Education, is a state-related institution of higher learning located in Western Pennsylvania. With an enrollment of over 35,000 students, the University is one of the largest institutions of higher education in Pennsylvania. Supporting its needs and interests are more than 13,200 faculty, research associates, and staff. The University's annual spending exceeds 1.74 billion dollars, of which approximately 700 million dollars are from sponsored research projects making the University one of the top tier research institutions in the country. The University is a member of the Council on Governmental Relations (COGR) and the Association of American Universities (AAU), and joins those organizations in their more detailed comments offered in this docket. These more specific comments are offered to emphasize the potentially significant, negative consequences of two specific definitional changes proposed in the above referenced docket.

The University of Pittsburgh welcomes the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32: Revisions to Definitions in the Export Control Regulations. We recognize and appreciate the work that the Departments of Commerce, State and Defense have placed into reforming the U.S. export control regulations, and believe that most of the proposed changes related to this revision are positive. For example, the exclusion of sending, taking, or storing software secured using end-to-end encryption from export activities is welcomed. This revision will reduce faculty burden associated with international travel and the need to monitor and conduct research using U.S. campus resources while overseas. We also note and applaud BIS's confirmation of our understanding of "fundamental research" at universities. We specifically cite the clear statement that a short pre-publication review of the results of fundamental research by sponsors to ensure that publication

Ms. Hillary Hess

July 31, 2015

Page 2

does not compromise patent rights (§734.8(b)(1)) or to insure that the publication does not inadvertently divulge sponsor provided proprietary information (§734.8(b)(2)) does not make the research subject to the Export Administration Regulations (EAR). However, as outlined in the comment letter submitted by COGR and AAU, several proposed changes would result in significant increased and new administrative burdens in the management of industry-sponsored research at universities.

Changes to Educational Information

Currently, under the EAR section §734.9, “educational information” is defined as information “released by instruction in catalog courses and associated teaching laboratories of academic institutions” while section §734.3(b)(3)(iii) excludes such information from the EAR. The proposed rule removes §734.9 and this definition, and replaces it in proposed EAR §734.3(b)(3)(iii) with information and software that “concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory at an academic institution”. We feel that this proposed change narrows the definition of educational information which is currently excluded from the EAR and contrary to the intent of the proposed final rule. It is quite common for universities to create new courses that include new and innovative content based on evolving technologies. It is not clear under the proposed change if this new content would be viewed as falling under general principles or commonly taught which would place it outside of EAR jurisdiction. The University of Pittsburgh’s enrollment procedures are non-discriminatory and its courses are open to anyone, regardless of citizenship or national origin, who have completed proper prerequisites. A narrow interpretation of the proposed revised EAR §734.3(b)(3)(iii) would inhibit the ability of U.S. universities to develop new courses that include innovative or novel content in new areas of science and engineering. This would have a direct downstream effect on the number of professionals trained in these areas and then available to new or existing U.S. business sectors.

The University of Pittsburgh is committed to maintaining openness in the dissemination of research results, consistent with the University’s non-profit mission of sharing knowledge. This commitment is codified in several University research policies, including those that address publication rights, employment opportunities, and commercialization of technology. For example, the University does not accept research awards that contain publication restrictions (beyond brief delays for intellectual property protection), or foreign national exclusion clauses. Moreover, University faculty and staff may not participate in any externally sponsored project where the results are restricted for proprietary or national security concerns.

Ms. Hillary Hess

July 31, 2015

Page 3

The University of Pittsburgh recommends that BIS keep the current phrase “released by instruction in catalog courses and associated teaching laboratories of academic institutions” for proposed section EAR §734.3(b)(3)(iii) and remove the proposed phrase “concern general scientific, mathematical, or engineering principles commonly taught in schools”.

“Fundamental research,” “technology,” and “software”

Publicly available technology and software arising during, or resulting from, fundamental research are not currently subject to the EAR (§734.3(b)(3)). Under the proposed EAR §734.8(a), “technology,” but not software, that arises during, or results from, fundamental research and is intended to be published, is not subject to the EAR. This is a significant change that will complicate and restrict university research. Both “software” and “technology” resulting from university research are published. Under the proposed change, a natural-language document written by a researcher could be “technology” arising during fundamental research while a computer-language document could be subject to deemed export restrictions, even though it arises during fundamental research and is intended to be published. We suggest that the language be revised to distinguish between source code, which may be published as the result of fundamental research, and other software.

On the other topics proposed in this docket, the University fully supports the positions outlined in the COGR-AAU comment letter. The University of Pittsburgh is appreciative of the opportunity to provide comments on these proposed changes.

Sincerely,



Allen A. DiPalma, MBA
Director, Office of Export Controls Services
Export Controls Official

Vice Chancellor for Research

August 3, 2015

Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, DC 20230

RE: Revisions to Definitions in the Export Administration Regulations (RIN 0694—AG32)

Washington University in St. Louis (WUSTL) is a private educational, research, and clinical institution with a long-standing commitment to the discovery of new knowledge and its translation for the public's benefit. The FY2014 WUSTL research portfolio of \$532M includes \$393M of funding from federal sources.

Our research enterprise engages faculty, staff, students, and trainees in a variety of activities and training programs across a broad spectrum of disciplines and our portfolio is increasingly supported by or performed in conjunction with national and international partners from other universities, national laboratories, foundations, and industry. WUSTL and other universities that engage in federally-sponsored research are increasingly encouraged by government programs and policies to urge our researchers, physicians, and scientists to be more entrepreneurial and aggressive to identify opportunities to transform the results of fundamental research into more developed concepts and commercially viable products.

All of this makes for an exciting and complex environment in which to conduct research, but it also makes it critically important for the many federal policies that shape that environment to be thoughtfully crafted, implemented, and enforced.

The Administration's Export Control Reform Initiative has been a welcome exercise. WUSTL recognizes and appreciates the substantial efforts to revise the Export Administration Regulations (EAR) and International Traffic in Arm Regulations (ITAR) by the Commerce Bureau of Industry and Security (BIS) and the State Department Directorate of Defense Trade Controls (DDTC). In particular, harmonized definitions between the EAR and ITAR would be helpful and significant, so the opportunity to comment on the proposed definitions is greatly appreciated.

WUSTL strongly supports and associates itself with the comments submitted by the Council on Governmental Relations (COGR), Association of American Universities (AAU), and the Association of Public and Land-grant Universities (APLU).

The area of greatest concern to WUSTL is a change that would cause common university research to lose its fundamental research presumption.

Vice Chancellor for Research

We strongly urge BIS to ensure that software resulting from research remains covered by the fundamental research exemption. Proposed changes to EAR do not treat software resulting from research, which is a document written in computer language and intended for broad based and open public dissemination, in the same manner it treats other research publications. This odd distinction is unnecessary for the purposes of the fundamental research exemption from export controls.

The COGR, AAU, and APLU comments are expansive on this and other important matters. The University hopes that the BIS will consider them as it finalizes the proposed definitions. Thank you again for the opportunity to comment and for your Export Control Reform Initiative efforts.

Sincerely,



Jennifer K. Lodge, PhD
Vice Chancellor and Associate Dean for Research



OFFICE OF THE VICE PROVOST FOR RESEARCH

Cumnock Hall
One University Avenue
Lowell, MA 01854

Phone: 978-934-2226
Fax: 978-934-3075
E-mail: Julie_Chen@uml.edu

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave., NW
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am writing on behalf of the University of Massachusetts Lowell (UML) concerning the proposed Revisions to Definitions in the Export Administration Regulations (EAR). UML is among the top 200 research universities in the U.S. (U.S. News & World Report), with total research and development expenditures of \$65 million annually. The UMass System is also ranked 13th in the U.S. for intellectual property generated.

The proposed Revisions to Definitions in the Export Administration Regulations (EAR) and corresponding changes to the International Traffic in Arms Regulations (ITAR) will, if adopted as proposed, have significant impact on academic institutions in the U.S. We appreciate the opportunity to comment on these revised definitions.

Changes to Educational Information

The current §734.9 defines “educational information” as information released by instruction in catalog courses and associated teaching laboratories of academic institutions, and §734.3(b)(3)(iii) excludes such information from the scope of the EAR. In the proposed rule, the definition of “educational information” is removed, and §734.3(b)(3)(iii) instead excludes information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution. We believe that the proposed change adds uncertainty and potentially narrows the scope of applicability of the exclusion. *A narrow interpretation of the revised §734.3(b)(3)(iii) could inhibit the ability of U.S. universities to develop new courses in emerging areas of science and engineering critical to employability of our graduates and the future competitiveness of the industrial sector.* UML recommends that the qualifier “concern general scientific, mathematical, or engineering principles commonly taught in schools” be removed and that the simpler “is released by instruction in catalog courses and associated teaching laboratories of academic institutions “ be retained for §734.3(b)(3)(iii).

Definition of “Fundamental Research”

The proposed definition of “fundamental research” using the language of NSDD-189 in the EAR is consistent with U.S. academic institutions’ understanding of the concept. The proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18), with an alternate definition adopting OMB Circular A-11 language. The OMB Circular A-11 language reads: “applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met”. This language is well understood by

universities in the context of reporting on federal expenditures to NSF, and UML supports the adoption of this commonly used definition.

BIS has also proposed an alternate definition: “fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. We assume that this simpler definition would not alter other wording in the proposed rule permitting prepublication review under specific circumstances within the fundamental research domain. While we generally favor the simplified definition, it would be helpful if a note were added to illustrate what is and is not non-proprietary, or alternately for the term to be defined.

UML appreciates that the proposed definition of “fundamental research” clarifies the broad applicability of the concept regardless of organization type or location. However, the removal of the specific criteria for university based research currently found in §734.8(b) creates interpretive uncertainty. U.S. universities use §734.8(b) to make determinations as to the applicability of fundamental research by evaluating proposed research activities using paragraphs 2 -6, and assume that the research qualifies as “fundamental research” if all conditions are met. *UML recommends that the specific language of §734.8(b) be retained in the EAR.*

“Fundamental research”, “technology”, and “software”

Under the proposed §734.8(a), “‘technology’” that arises during, or results from, fundamental research and is ‘intended to be published’” would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR.

The proposed rule refers to a proposed note “to clarify that software and commodities are not ‘technology resulting from fundamental research’” (although we were unable to locate the note). *This change would significantly complicate and restrict university research.* While natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to export restrictions. “Software” resulting from university research is “published” as well as “technology”, as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology. *UML strongly recommends that the proposed §734.8(a) be revised as follows:*

§ 734.8 “Technology” and “software” that arises during, or results from, fundamental research.

(a) “Technology” or “software” that arises during, or results from, fundamental research and is ‘intended to be published’ is not ‘subject to the EAR.’”

Questions and Answers- Technology and Software Subject to the EAR

UML urges BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. While we agree that the questions and answers are illustrative, inclusion of them in the EAR removes the uncertainty created by changes due to interpretive differences without benefit of the rulemaking process. We are concerned that removal of the questions and answers, which are widely used by industry and academia to guide export control decisions, would create increased uncertainty in our application of key concepts, including fundamental research, publication, and educational instruction.

End to End Encryption Standard

The addition of §734.18 listing activities that are not exports, re-exports, or transfers is a useful addition to the EAR. *In particular, the exclusion of sending, taking or storing software that is secured using end to end encryption from export activities is welcome to the academic research community, as it will reduce*

the faculty burden associated with external collaborations and off-site research activities. UML supports the proposed EAR illustrative standard of FIPS 140-2, supplemented in accordance with NIST guidance or other similarly effective means.

UMass Lowell appreciates the opportunity to provide comments on these proposed changes and would be happy to discuss in further detail if helpful.

Sincerely,

A handwritten signature in blue ink that reads "Julie Chen". The signature is fluid and cursive, with the first name "Julie" and last name "Chen" clearly legible.

Julie Chen

Vice Provost for Research

**Yale OFFICE OF THE VICE PRESIDENT
AND GENERAL COUNSEL**

PO Box 208255
New Haven CT 06520-8255
T 203 432-4949
F 203 432-7960
courier
Whitney Grove Square
2 Whitney Avenue, 6th Floor
New Haven CT 06510

August 3, 2015

Ms. Hillary Hess
Director
Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230

Dear Ms. Hess:

I write on behalf of Yale University to comment on the Bureau of Industry and Security's (BIS) proposed revisions to the definitions in the Export Administration Regulations (EAR).

Yale applauds this important effort to make the language and structure of EAR and the International Traffic in Arms Regulations (ITAR) more consistent, thereby achieving greater harmonization of two distinct regulatory regimes. In general, we believe this is a positive step toward implementation of the Administration's Export Control Reform Initiative – and the ultimate export control objective of creating a common set of regulations. With careful construction and implementation, these reform efforts will enhance national security and facilitate compliance while reducing related costs and burdens for exporters, including Yale.

We appreciate that most of the proposed revisions would not substantively change the existing rules. Instead, they would create substantive and structural harmonization, using the same words for the same concepts in the EAR and ITAR and similar definitions in a common format that helps make the differences clear. In particular, we support proposed inclusion of the definition of fundamental research proposed by the BIS in Section 734.8(c), which is identical to the National Security Decision Directive (NSDD) 189. To smooth implementation and aid in compliance, we suggest revisions or clarifications to the sections concerning the end-to-end encryption standard, the definitions of "technology" and "software," and the contract controls for government-sponsored research.

Fundamental Research Definition

We support the proposed definition offered by BIS for 'fundamental research', which we believe is identical to the definition in NSDD-189. Specifically, in Section 734.8(c), 'fundamental research' means "basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." The use of this definition in the EAR and the ITAR would be most consistent with our understanding of

the term. We also believe this is an improvement over the alternative proposed definition, in which 'fundamental research' means "non-proprietary research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community." We are concerned that the alternative definition relies on undefined or vague terms. For example, the term 'non-proprietary' could be defined to mean several different things, including unprotected by patents, copyrights or trademarks or existing in the public domain.

Fundamental Research and Software

Currently, the EAR, in Section 734(b)(3), states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. Yet, as proposed in Section 734.8, only 'technology' that arises during, or results from, fundamental research and is 'intended to be published' would not be subject to the EAR. Further, the preamble discussing this section states that the "proposed notes clarify that...software and commodities are not 'technology resulting from fundamental research.'" In other words, in the above referenced sections, software appears to be no longer covered by the fundamental research exception.

Notwithstanding these sections, the general section on exclusions would seem to contradict the proposed narrowing of the fundamental research exception, creating tension and confusion. Specifically, proposed Section 734.3(b)(3) states that "information and 'software'" are not subject to EAR if they arise during, or result from, fundamental research, as described in Section 734.8.

If software arising during, or resulting from, fundamental research were no longer subject to the fundamental research exception, research at Yale would be significantly constrained. Natural language documents written by a researcher may be considered "technology" while a computer language document written by the same researcher may be considered "software." Despite the fact that both arise during fundamental research and are written for the purpose of being freely shared, the technology would be considered exempt while software would be subject to deemed export restrictions. This conclusion would be at odds with the fact that much of science involves the creation of software. If such software were no longer covered by the fundamental research exception, Yale would have to treat the research itself as not covered, undercutting the value of the exception and potentially subjecting much of our research to export controls. Given that the export definitions in Section 734.2(b) recognize the similarities between software and technology, and the confusion that this change will likely cause, we strongly recommend that software arising during, or resulting from, fundamental research remain covered by the fundamental research exception.

Further, we have noticed that the current presumption in EAR 734.8(b), that university-based research is considered fundamental research, appears to have been eliminated. Absent a clear policy reason for this change, we urge you to restate the presumption in the final rule.

Transfer and Storage

The proposed rule clarifies that when technology/technical data or software is transmitted electronically through, or stored electronically in, a foreign country, an export, reexport, or (re)transfer has not occurred if the technology/technical data or software is unclassified; it is encrypted end-to-end; it is secured using modules compliant with FIPS 140-2 and supplemented

by other controls consistent with NIST guidance; and, in the case of technical data under ITAR or controlled technology or software under EAR, it is not stored in a proscribed country listed in Section 12.1 or in Country Group D-5 or in Russia.

We greatly appreciate the proposed rule's clarification that the transmission of unclassified technical data through a foreign country's Internet service infrastructure does not require a license, provided that the technical data is encrypted prior to leaving the sender's facilities and remains encrypted until received by the intended recipient. Similarly, we appreciate that the electronic storage abroad of encrypted technical data would not require an authorization. As you have recognized, ITAR controlled technical data may be electronically routed through foreign servers without the knowledge of the original sender. For example, an email may, without the sender's knowledge, transit a foreign country's Internet service infrastructure en route to its intended destination. Or data intended for cloud storage may, without the sender's knowledge, be physically stored on a server located in a foreign country (or multiple foreign countries). This creates a risk of unauthorized access and a potential for an inadvertent ITAR violation, which the proposed rule seeks to mitigate.

Even with the improvements in the proposed rule, we are concerned that the end-to-end encryption requirement will create significant compliance challenges for institutions that rely on third party vendors for these services. As stated above, these servicers might encrypt and decrypt information at various points in the process of transmitting or storing technology or software, potentially triggering an export or reexport that would require BIS authorization. Although not explicitly stated in the proposed rules, the end-to-end encryption requirement seems to imply that the owner of the data or software (the sender), not the vendor, would be responsible for any unauthorized transmission or release of controlled technology or software. Given that vendors ultimately will be responsible for refining their offerings to ensure that data is not decrypted at any time and that no servers are located in restricted countries, we urge you to consider the creation of a safe harbor for senders that impose a contractual obligation on the vendor to comply with these transmission and storage requirements.

In addition, with respect to the intended control, we prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur.

Ultimately, the usefulness of the transfer and storage provisions in the proposed rule will be limited by the prohibited countries list. We strive to clearly understand what is going to happen to our data once it is in the cloud (i.e. what data will be uploaded, transferred or downloaded from the cloud, and when and by whom) and we take steps to ensure that providers put appropriate measures in place to prevent unauthorized access, but many large providers are unwilling to tell users where their clouds are located or on which clouds data is stored. Given that the burden of compliance rests with the sender, not the provider of the cloud computing services, the inclusion of China in a prohibited county list would effectively preclude U.S. institutions and companies from using cloud storage. We urge you to consider a narrower prohibited countries list – such as the Office of Foreign Assets Control embargoed countries list – that, together with end-to-end encryption, will provide adequate protection without requiring compliance with mandates that are outside of the sender's primary control.

Contract Controls/Government Sponsored Research

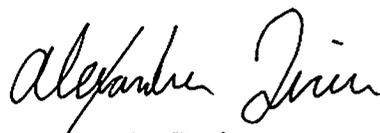
Currently, Section 734.11 provides: "If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provision of Section 734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific national security controls may nonetheless be made under this provision." The proposed EAR rule restates the current 734.11(a), which always has been a source of confusion, with the meaning of "this provision" in the last sentence unclear.

The Q&A embedded in the current regulations make clear that any export "that is consistent with the controls will continue to be eligible...under the 'fundamental research' rule." (Supplement No. 1 to Part 734, Question E(1)) With the Q&A being moved out of the regulation, we believe it is important to make sure that Section 734.11 is unambiguous. Therefore, we suggest the following modification:

"If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provision of Section 734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific national security controls may nonetheless be made under Section 734.3(b)(3)."

Again, we appreciate this opportunity to comment. We look forward to working with you to preserve the U.S. leadership position in science and technology and to advance the national security.

Sincerely,



Alexander Dreier
Vice President and General Counsel



GE

Kathleen L. Palma
Senior Executive
International Trade Compliance
GE Corporate Legal – ITC COE

1299 Pennsylvania Ave NW
Washington, D.C. 20004-2414
United States of America

T 202 637 4206
kathleen.palma@ge.com

August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C.

Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C.

Regulation IDs: RIN 1400-AD70 and RIN 0694-AG32

Subject: Comments on Proposed Revisions to Definitions in the International Traffic in Arms Regulations and the Export Administration Regulations

Dear Mr. Peartree and Ms. Hess:

General Electric Company (GE) submits the following comments in response to the Department of State, Directorate of Defense Trade Controls' (DDTC's) and the Department of Commerce, Bureau of Industry & Security's (BIS's) June 3, 2015 Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), (80 Fed. Reg. 31, 525 and 80 Fed. Reg. 31, 505) (Proposed Rules). GE welcomes the opportunity to comment on the Proposed Rules.

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "EXPORT"

Comments related to the revised definition of the term "Export" in ITAR §120.17 and EAR §734.13 and Activities that are Not Exports, Reexports, Releases, Retransfers, or Transfers in ITAR §120.52 and EAR §734.18

GE supports the proposed exclusions from the definitions of export for data that is secured by encryption as described in the Proposed Rules. This mechanism will provide some additional

flexibility for exporters who operate in multinational IT environments without compromising the security of the controlled data. In addition, the ability to store data outside of the U.S. will result in the ability to use lower-cost cloud options than U.S.-only cloud storage solutions. The ability to host the data closer to the customer will also improve access times globally. These benefits are substantial and the proposals represent a significant step for the U.S. Government to recognize that national borders are not the most important consideration for data security.

However, GE does have several concerns about the proposals as currently drafted. First, the requirement to use end-to-end encryption will be costly, difficult to implement and will reduce application functionality in systems that have reporting or analytic sub systems. In practice, the end-to-end encryption requirement will limit the utility of the proposal for storage of data and possibly bilateral exchange of data and will not allow the proposal to be used for other data uses. Today GE uses end-to-end encryption only in specific use cases because of the complexity involved in having the employee encrypt the data with a private key. We typically utilize environments that have strong external data security protections but do not normally require the use of end-to-end encryption. There are many other ways to protect data without the use of end-to-end encryption. If the final rules broadened this requirement to require the use of secure encryption to protect the data at all times without a specific requirement for end-to-end encryption, it would have far more utility.

Second, GE is concerned that the proposed definition of "end-to-end encryption" requires the means to access the data/keys not be given to any party other than the intended recipient. In this respect, the definition goes well beyond what is required to ensure that the data is not released to a non-U.S. person. It would be far preferable to limit the requirement not to share the data/keys with non-U.S. persons; sharing with a U.S. person IT professional inside the U.S. should not void the ability to use the provision.

Third, GE utilizes SSL Inspection Tools that decrypt data in transit, scan it for malicious code, and then re-encrypt the data with a dummy token that allows it to be passed on to the intended recipient. Without this decryption process, the malicious code inspection could not occur, potentially creating data security risks. While we have the ability to prevent data from going through one of the SSL inspection tools, our ability to prevent the data from going through another party's inspection tools is uncertain.

Fourth, with regard to the encryption standard that is authorized, GE prefers the proposed formulation in the EAR versus the ITAR in that it allows, in addition to cryptographic modules compliant with FIPS 140-2 and supplemented by procedures/controls in accordance with NIST publications, "other similarly effective cryptographic means." This standard will allow exporters to utilize a broader range of tools that will provide strong protection to controlled data. In fact, it is quite possible to be more secure than FIPS 140-2 or to be FIPS 140-2-equivalent without being FIPS certified. The NIST certification is sometimes constrained by time, and some vendors also do not wish to incur the cost. It can take six to nine months and several hundred thousand dollars to be FIPS 140-2 certified. Some software vendors, while clearly meeting the standard in practice, do not spend the time and money on such a certification. GE therefore urges the agencies to harmonize around the EAR formulation since companies that work with both ITAR and EAR data will be driven to the most restrictive standard.

The Proposed Rules restrict the countries in which controlled data can be stored, prohibiting storage of controlled data in EAR Country Group D:5 and Russia and ITAR 126.1 countries. GE requests clarification on whether data that is sufficiently encrypted to meet the requirements outlined in this Proposed Rule and that is "routed through", rather than "stored in", an EAR Country Group D:5 country, Russia, or an ITAR §126.1 country similarly would not be released from control under EAR §734.18 or ITAR §120.52.

Comments on definition of "Export of Technical Data" in ITAR §120.17(a)(6)

This section states:

§120.17 Export

120.17 (a)(6) - "Releasing or otherwise transferring information such as decryption keys, network access codes, passwords, or software, or providing physical access, that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred ..."

We recommend that the underlined language be revised to align the ITAR definition with the EAR definition, by incorporating concepts of "knowledge" and "actual transfer" into the definition. We suggest the following rewrite:

120.17(a)(6) - "Releasing or otherwise transferring decryption keys, network access codes, passwords, software or other information with knowledge that such provision will result in the transfer of other technical data in clear text (i.e., in unencrypted form) or software (i.e., in source code format) to a foreign person."

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "TECHNICAL DATA" AND "REQUIRED"

Comments on ITAR Proposed Rule related to use of the term "technical data" in defining "required" in §120.46

GE believes that ITAR §120.46(a) may be confusing to many users because it indirectly uses the term "technical data" to define the term "technical data." In §120.10(a)(1), "technical data" is defined in terms of information required for certain defined activities. But in §120.46(a), "required" is proposed to be defined as technical data peculiarly responsible for certain controlled parameters. Since the term "required" is used in the context of identifying which information will be controlled as technical data under the ITAR, GE believes the definition would be clearer if it were modified as follows. (underscored to show changes):

"As applied to technical data, the term required refers to only that portion of information that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions. Such required information may be shared by different products."

Conforming changes should also be made in each of Notes 1, 2 and 3 to paragraph (a).

Comments on ITAR Proposed Rule related to use of clarifying example in defining "required" in §120.46

In the EAR, the definition of "required" includes an example to help clarify that certain technology, although used in a controlled item, is not intended to be controlled because its use relates to the achievement of characteristics that are common to other commodities that are not controlled. GE believes that the ITAR should include a similar example so that information that may be useful in the development of a defense article but which has broader civil and commercial applications is not controlled. We propose that an example such as the following be included in §120.46(a):

"... performance levels, characteristics, or functions. Such "required" information may be shared by different products. For example, assume product "X" is controlled if it is capable of operating for sustained 30 second inverted flight, and is not controlled if is merely designed to sustain an emergency flight inversion for a few seconds. If the information used in development includes technologies "A", "B", and "C" which allow inverted flight as an emergency measure but not for more than 10 seconds, then technologies "A", "B", and "C" are not "required" to develop the controlled product "X." If technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can develop a product "X" that is capable of operating for sustained 30 second inverted flight. In this example, technologies "D" and "E" are "required" to make the controlled product."

Comments related to use of the term "peculiar to" in defining "required"

GE believes that using the phrase "peculiar to" in the notes to the definition of "required" (Note 1 to paragraph (a) in the ITAR, and Note 1 to the definition of "required" in the EAR) is confusing because of its similarity to the defined term "peculiarly responsible." If it is intended to mean the same thing, then GE suggests replacing the phrase "peculiar to" with "peculiarly responsible for." If the intended meaning is different than the specialized "peculiarly responsible for" term, we would alternatively recommend replacing "peculiar to" with "unique and specific to," in order to avoid confusion.

Comments related to the definition of "peculiarly responsible"

GE believes that the catch and release approach taken to define "peculiarly responsible" is one which industry will find familiar and helpful. However, we are concerned that strictly following the model used in the definition of "specially designed" results in over-regulation of information used in applications that are not military in nature. We are particularly concerned with information that has no relationship to the parameters (e.g., performance levels, characteristics, functions or other essence such as being a bomber) that cause the item to be controlled. To align this catch and release mechanism with the concept expressed in the example to the EAR definition of "required" (i.e., A, B, C, D and E), GE proposes the following 2 changes:

- 1) Change the "catch" paragraph of the definition as follows: "... is "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" if it is used in or for use in the development ... or refurbishing of the controlled parameters or portions of the item that incorporate the controlled parameters of a [defense article/item subject to the EAR] unless ..."

- 2) Add the following wording as release paragraph no. 2: "It is directly related to an item that is a part, component, accessory, attachment or software used in or with the defense article or item subject to the EAR that is the object of the first paragraph of this [Note/Definition];"

In addition, under the strict limitations of release paragraph no. 3, which require information to be both identical and used specifically in production items as conditions for release, a simple dimension difference between a bracket having no military functionality that is used on a military item and another bracket used on a commercial item (non-production) will be controlled even though all information and data used to design the dimensional differences themselves are commonly used in civil, non-military designs. Thus a license might be required to have this simple bracket made. GE proposes incorporating the "or equivalent" concept from the "specially designed" definition by modifying release paragraph no. 3 and adding a new Note as follows: "Is identical or equivalent in form and fit to information used in or with a commodity or software that . . ."; "Note 1 to release paragraph no. 3: With respect to information, "equivalent" means its differences relate solely to the form and fit of the commodities it is used with."

Comments related to Potential Conflict between Notes 2 and 3 to paragraph (a) of §120.46

GE believes there is a potential conflict between Notes 2 and 3 to ITAR §120.46.a. If a component subject to the EAR and under development (not in production) is incorporated or installed in a Defense Article, Note 2 indicates that the jurisdictional status of technical data directly related to development of that component is the same as the component and is not controlled under the USML. But under the catch and release mechanism of Note 3, the same technical data would be "peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions" because it is used in or for use in the development of the defense article into which the component is incorporated and there is no applicable release paragraph. As GE believes the U.S. Government's intent is to exclude technical data unless it is directly related to the controlled defense article, and not merely used in the article, GE suggests that the following words be inserted in the beginning of Note 3: "Except as described in Note 2 to paragraph (a), technical data is "peculiarly . . ."

Comments on ITAR Proposed Rule related to definition of the term "knowledge"

In Note 3 to paragraph (a) of §120.46(a), the term "knowledge" is used as an element for releasing technical data under release paragraphs 4 and 5. The use of this term for such release purposes is similar to its use in §120.41 ("specially designed") where Note 2 to Paragraphs (b)(4) and (5) defines knowledge. But that definition of "knowledge" is expressly limited to §120.41. GE recommends duplicating that definition as a new Note to Note 3 to paragraph (a) of §120.46(a). GE does not believe, however, that "knowledge" should be a separate Part 120 definition, as "knowledge" has a number of other uses in the ITAR, such as in Part 127, that have come to be understood for other specialized purposes.

Comments related to placement of the definition of "peculiarly responsible"

Comments were requested on the placement of the definition of "peculiarly responsible" in a Note to the definition of "required" versus as a stand-alone definition. GE agrees with DDTC's choice to limit its applicability to the concepts contained in §120.46. The definition of "peculiarly responsible" was

obviously given a lot of thought and written for the description of controlled technical data. The other place where the concept of "peculiarly responsible" is used is in the definition of "specially designed." The "specially designed" definition uses the term to describe properties of commodities or software to determine whether items having those properties are "specially designed." If a common definition were created, in one place it would describe an item (technical data) and in the other a non-item (properties). We are concerned that this will cause confusion for several reasons. First, there would be two distinct catch and release mechanisms operating within the "specially designed" definition, which is already complex and difficult to understand (one to determine if an item is caught under the "specially designed" part (a)(1) catch test, and the other for the "specially designed" part (b) release test). Second, use of the definition in "specially designed" would result in the anomaly of having some of the releases currently operating under part (b) of "specially designed" and adopted for the "peculiarly responsible" releases, applying to end items and materials, where those part (b) "specially designed" releases were originally intended to not apply to end items or materials.

GE also recommends that the definition of "peculiarly responsible" be removed from Part 772.1 of the EAR, and placed as Note 3 to the definition of "required."

COMMENTS PERTAINING TO THE PROPOSED DEFINITION OF "DEFENSE SERVICES"

While GE supports the clarifications and changes proposed by DDTC to the definition of "defense services" as major improvements to the earlier proposed definition, we believe that additional clarifications are necessary before a final rule is implemented.

Comments on ITAR Proposed Rule related to §120.9(a)

Use of knowledge of technical data to determine whether a defense service has been provided. GE is deeply concerned about the attempt to define defense services based on the "knowledge" of relevant technical data by the U.S. person. It is highly problematic to establish this standard based on what an engineering resource may have contained in his/her brain. This could set up truly difficult enforcement cases that do not hinge on what was actually provided to the non-U.S. entity that received the service but the knowledge of the engineer or service technician involved in providing the service. GE submits the knowledge of the individual involved should not be dispositive in determining whether a "defense service" has been provided, but rather the rules must focus on what benefits the non-U.S. entity received related to the defense article(s).

ITAR Proposed Rule Use of the term "participate." If the DDTC does not remove the knowledge requirement from the definition as suggested above, GE has additional concerns about the proposed approach. Specifically, pursuant to Note 1 to paragraph (a)(1) a person is deemed to have "knowledge of U.S.-origin technical data" directly related to a defense article if the person participated in the development of a defense article. GE believes that using participation as the threshold for determining whether a person has knowledge that rises to the level needing control as a defense service would result in the regulation of a broader set of persons than is necessary. A plain dictionary meaning of the word "participate" is "to take part in an activity." Under this definition, "participation" can include remote and indirect involvement insignificant to the actual development activities, including medical, logistical, translation, financial, legal, scheduling, and administrative services. GE proposes that the scope of deemed knowledge be narrowed to those activities that are directly related to the development activities. One way to narrow this scope would be to modify the

second sentence of Note 1 to paragraph (a)(1) to state: “. . . However, a person is deemed to have knowledge of U.S.-origin technical data directly related to a defense article if the person engaged in activities directly related to the development of a defense article . . .”

ITAR Proposed Rule Reference to Defense Articles in the same USML paragraph. Note 1 to paragraph (a)(1) would deem a person to have “knowledge of U.S.-origin technical data” if their prior activities related to development of any defense article described in the same USML paragraph as the article that is subject of the assistance. GE believes this is also too broad because it would include involvement in the development of prior items that may have no relevance to the present assistance. For example, a person may have been involved in development of a gas turbine engine design 30 years ago (such as the J79) involving technologies that have been superseded by several generations of new engine designs. That involvement would provide little to no applicability to an advanced engine such as the F135. In addition, given the length of time, the burden on both the company and the individual to consider “participation” that is so remote in both time and relevance to the current assistance (and may require research into the actual activity for which records and memories may be scant) exceeds any benefit that U.S. Government might obtain in regulating that assistance. GE proposes narrowing the scope of the defense articles used for comparison under this provision to those that have direct relevance to the activity. One way to narrow this scope would be to further modify the second sentence of Note 1 to paragraph (a)(1) to state: “. . . However, a person is deemed to have knowledge of U.S.-origin technical data directly related to a defense article if the person engaged in activities directly related to the development of portions or properties of a defense article that has the same properties, and is described in the same USML paragraph as, . . . the defense article that is subject of the assistance . . .”

Comments on ITAR Proposed Rule related to clarification regarding the exclusions in Note to paragraph (a)

Note to paragraph (a), item no. 2 adds little guidance and may cause confusion. This item no. 2 states that performance of services by a U.S. person in the employment of a foreign person is not a defense service “except as provided in this paragraph [i.e., 120.9(a)]”. Essentially, paragraph (a) provides a detailed description of what activities are defense services, and this item no. 2 states the obvious that if an activity is not described in paragraph (a) it is not a defense service. GE recommends that DDTC include examples or make a clearer statement of parameters that would be outside the scope of the description in paragraph (a). One approach could be to modify item no. 2 to state: “Performance of services by a U.S. person in the employment of a foreign person related to the production of a defense article without having the requisite knowledge described in Note 1 or Note 2 to paragraph (a)(1).”

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF “PUBLIC DOMAIN”

Comments on ITAR Proposed Rule related to definition of “public domain” in ITAR §120.11

GE believes that the requirement in ITAR §120.11(b) that the U.S. Government authorize all technical data or software that may be subject to the ITAR prior to release into the public domain may impose a prior restraint on the publication of privately generated unclassified information and violate the First Amendment of the U.S. Constitution. GE recommends that §120.11(b) be revised to apply only to specific types of information, such as government-funded or classified information.

Separate from the First Amendment concerns, GE questions the practicality of the proposed ITAR §120.11(b) requirement:

1. How will the Directorate of Defense Trade Controls, Office of Security Review or other relevant U.S. Government entity ensure authorization requests are processed promptly?
2. What factors will the U.S. Government rely on to determine whether authorization will be given for the release of technical data or software into the public domain?
3. How do exporters know which U.S. Government entities have the authority to issue the requisite approval for release of which technical data or software into the public domain under §§120.11(b)(3) or 120.11(b)(4)?

If DDTC proceeds with this proposed requirement notwithstanding the significant Constitutional and practical concerns, GE requests further clarity on the potential scope of §120.11(b)'s requirement. Note 1 to §120.11 states that §127.1(a)(6) prohibits the unauthorized export, reexport, retransfer or public release of technical data or software with knowledge that the technical data or software was made publicly available without the approval required in §120.11(b), but it does not address how technical data or information placed in the public domain without authorization prior to the effective date of this rule will be handled. It is simply unrealistic to require all technical data or software currently in the public domain without express U.S. Government authorization to receive U.S. Government authorization prior to further release, export, or reexport. GE recommends, at a minimum, the inclusion of a grandfathering clause to exempt technical data or software in the public domain prior to the effective date of the rule from §120.11(b) requirement and §127.1(a)(6).

Finally, GE requests a 6-month transition period to implement the required changes if the proposed change is finalized given the widespread effects of such a requirement.

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF "PERMANENT AND REGULAR EMPLOYEE"

Comments EAR Proposed Rule related to definition and use of "permanent and regular employee" in EAR §§734.20 and 750.7

GE disagrees with the proposed definition and use of the phrase "permanent and regular employee" in §§734.20 and 750.7(a) to require employment for one year or longer. In practice, the term "permanent and regular employee" generally is applied to contract or contingent workers in foreign facilities. Mandating a period of one year or longer for the relationship significantly compromises the ability of a non-U.S. defense company to take advantage of the provisions that use this phrase. Many companies do not employ contract workers for periods of a year or longer because doing so can create a risk under labor and employment law that the contract worker would take legal action to acquire the benefits and other rights of employees.

The five specific criteria enumerated under §734.20(d)(2) are adequate to ensure appropriate control of EAR data in that the worker must: (i) work at the company's facilities; (ii) work under the company's direction and control; (iii) work full time and exclusively for the company; (iv) execute nondisclosure

certifications for the company and (v) not be taking direction from the staffing company. Why is it necessary for the relationship to be "long term" if those criteria are satisfied? The company engaging the contract employee will be responsible for the conduct of the worker regardless. The company can decide the length of relationship that would be appropriate given these competing considerations.

Moreover, the timing requirement does not necessarily apply or make sense in other contexts. What if a company hires an individual for permanent employment and the employee quits after 30 days? There ultimately would be no "long term" relationship under those circumstances either, yet it is not clear in the proposed definition and use of the phrase whether the employee would fall under the "permanent and regular" definition after being hired.

GE also requests further clarification on how the proposed use of the phrase "permanent and regular employee" in §750.7 may impact existing licenses. BIS typically limits employees authorized to receive controlled data through the inclusion of conditions with the license but does not put a restriction on the amount of time an employee must be working at a facility. If the proposed changes to §750.7(a) are finalized, what happens to employees under existing licenses that do not meet the specified "permanent and regular employee" definition but were not explicitly limited in the license conditions?

GE strongly urges BIS to change the proposed language as follows:

§734.20 Activities that are not "deemed reexports."

(b) Release to A:5 nationals...

(1) * * *5 nationals...

(2) The foreign national is a regular ~~and permanent~~ employee...

(c) Release to other than A:5 nationals... R

(1) * * * ~~release to other than A:5 nationals.~~

(2) The foreign national is a regular ~~and permanent~~ employee...

(d) Definitions. ~~Definitions.~~

(1) * * *

(2) "~~Permanent and~~ is an individual who:

(a) Is ~~permanently (i.e., for not less than a year) and~~ directly employed by an entity, or

(b) Is a contract employee who:

(i) Is in a ~~long-term~~ contractual relationship with the company...

§750.7(a) ... A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity's foreign nationals who are ~~permanent and~~ regular employees (and who are not proscribed persons under U.S. law)...

COMMENTS PERTAINING TO THE PROPOSED DEFINITIONS OF “ACTIVITIES THAT ARE NOT DEEMED REEXPORTS”

Comments related to definition of “Activities that are not “deemed reexports” in EAR §734.20(c)

GE believes the requirement in §734.20(c)(5)(ii)(B) to screen for contacts in Country Group D:5 is too broad. Country Group D:5 includes countries such as China and Vietnam where, like many multinational companies, GE has major manufacturing operations and installation bases. As a result, many employees are likely to have “substantive contact” (as defined in §734.20(d)(1)) with these countries (e.g., “recent or continuing contact with agents, brokers, and nationals of such countries,” “maintenance of business relationships with persons from such countries”) as a normal course of business (not including technology or source code transfers). Implementation of the proposed requirement in §734.20(c)(5)(ii)(B) therefore would consume tremendous amounts of resources without yielding substantive screening results mitigating the targeted risks of diversion.

GE suggests that the requirement in §734.20(c)(5)(ii)(B) to screen for contacts in Country Group D:5 be revised to more specifically address the potential risk of diversion – e.g., change the requirement to screen for contacts in to Country Group E:1, or change the proposed language to:

§734.20 Activities that are not “deemed reexports.”

(d) Definitions. (1) “Substantive contacts” includes ~~regular travel to countries in Country Group D:5; recent or continuing contact with agents, brokers, and nationals of such countries;~~ continued demonstrated allegiance to such countries; ~~maintenance of business relationships with persons from such countries;~~ maintenance of a residence in such countries; receiving salary or other continuing monetary compensation from such countries; or acts otherwise indicating a risk of diversion.

In addition, GE finds the requirement in §734.20(c)(5)(iii)(D) to maintain records for the longer of five years or the duration of individual’s employment with the entity to be overly prescriptive and burdensome. GE suggests that BIS change the proposed language to:

§734.20 Activities that are not “deemed reexports.”

(c) Release to other than A:5 nationals.

(5) * * *

(ii) * * *

(D) Maintains records of such screenings for ~~the longer of five years or the duration of the individual’s employment with the entity;~~ five years after the release of “technology” or “source code” takes place.

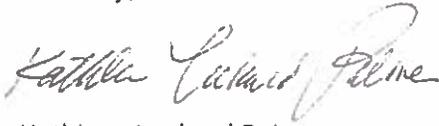
It is also worth noting that the requirements of §734.20(c)(5)(ii)(B) and 734.20(c)(5)(iii)(D) seem more restrictive than the riders and conditions with licenses that would cover the same foreign national employees from Country Group D:5. If the foreign entity can demonstrate effective compliance to §§734.20(c)(3) and 734.20(c)(4), then §§734.20(c)(5)(ii)(B) and 734.20(c)(5)(iii)(D) have very little value

considering the extra burden beyond a typical license. Given the personal data privacy laws in Europe and Canada, compliance with §§734.20(c)(5)(ii)(B) and 734.20(c)(5)(ii)(D) is even more difficult.

* * * * *

We appreciate the opportunity to provide comments on the Proposed Rules. If you have any questions or require additional information concerning this submission, please contact the undersigned at (202) 637-4206 or by email at: kathleen.palma@ge.com or George Pultz at (781) 594-3406 or by email at: george.pultz@ge.com.

Sincerely,



Kathleen Lockard Palma
International Trade Compliance

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security (BIS)
14th Street and Pennsylvania Ave. NW.
Room 2099B
Washington, DC 20230

RE: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32)

Dear Ms. Hess,

I am writing on behalf of the University of Michigan (“U-M”), a public, nonprofit, educational institution. The U-M conducts a high volume of diverse research activity and has faculty, students, and staff from all over the world. We appreciate the opportunity to comment on the proposed *Revisions to Definitions in the Export Administration Regulations* (80 Fed. Reg. 31505, June 3, 2015). The proposed revisions to the Export Administration Regulations (EAR) and corresponding changes to the International Traffic in Arms Regulations (ITAR) could, if adopted as proposed, have significant impact on research and education at the U-M. We believe there are significant opportunities for the U.S. Department of Commerce to revise these definitions further to achieve greater harmonization and to avoid revisions that could have a negative impact on U-M’s research enterprise.

Definition of “Fundamental Research”

The proposed definition of “fundamental research” using the language of NSDD-189 in the EAR and the ITAR is consistent with our understanding of the concept. BIS has also proposed a simpler, alternate definition that would read:

“Fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.

We assume that this simpler definition would not alter other wording in the proposed rule permitting prepublication review under specific circumstances within the fundamental research domain. While we find the simplified definition acceptable, it would be helpful if a note were added to illustrate what is and what is not “non-proprietary research,” or alternately for the term to be defined to allow for prepublication review by a research sponsor.

While the proposed definition of “fundamental research” clarifies the broad applicability of the concept, the removal of the specific criteria for university-based research found in the current §734.8(b) is confusing. The U-M has used §734.8(b) to make determinations as to the applicability of fundamental research by evaluating proposed research activities against paragraphs two through six. We assume that its research qualifies as “fundamental research” if all conditions are met. We strongly recommend that the specific language of §734.8(b) be retained. If this is not possible, we suggest that BIS develop a decision tree tool for the determination of fundamental research for universities that incorporates the current criteria for university based fundamental research.

Changes to Educational Information

The current §734.9 defines “Educational information” as information “released by instruction in catalog courses and associated teaching laboratories of academic institutions,” and the current §734.3(b)(3)(iii) excludes such information from the scope of the EAR. In the proposed rule, the definition of “Educational information” is removed. The proposed §734.3(b)(3)(iii) adds uncertainty and potentially narrows the scope of applicability of the exclusion for the U-M. If the U-M is contemplating new curricular additions, would we need to concern ourselves that the course may not be “commonly taught” at other universities? Many catalog courses include hands on design laboratories, particularly as capstone experiences. Would the content of these courses, which would have previously been treated as “educational information,” now become subject to the EAR by virtue of including more than general principles?

The U-M does not discriminate on the basis of citizenship or national origin in academic programs. Education at universities is by nature open, with the opportunity to participate limited only by fulfillment of required prerequisites. A narrow interpretation of the revised §734.3(b)(3)(iii) would inhibit the ability of the U-M to develop new courses in emerging areas of science and engineering critical to employability of their graduates and the future competitiveness of the industrial sector. We recommend that the qualifier “concern general scientific, mathematical, or engineering principles commonly taught in schools” be removed and that the simpler “is released by instruction in catalog courses and associated teaching laboratories of academic institutions” be retained for §734.3(b)(3)(iii). As an alternative, we believe changing the proposed description to “information and ‘software’ that concerns general scientific, mathematical, or engineering principles commonly taught in schools and/or released by instruction in a catalog course or associated teaching laboratory of an academic institution” would describe educational information more fully without narrowing the scope of the exclusion.

“Technology” and “Software”

Under the proposed §734.8(a), “Technology” that arises during, or results from, fundamental research and that is “intended to be published” would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR. This change would significantly complicate and restrict U-M’s research because while natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document (source code) written by the same researcher would be subject to deemed export restrictions. We strongly recommend that the proposed §734.8(a) be revised as follows:

Proposed revised language for §734.8

Revise title to: “Technology” and “software” that arises during, or results from, fundamental research.

(a) “Technology” or “software” that arises during, or results from, fundamental research and that is ‘intended to be published’ is not “subject to the EAR.”

(b) Prepublication review. “Technology” or “software” that arises during, or results from, fundamental research and that is “intended to be published” to the extent that the researchers are free to publish the technology and software source code without restriction or delay.

“Technology” that arises during, or results from, fundamental research subject to prepublication review is still “intended to be published” when...

Omission of software from the definition of “Technology” would significantly complicate and restrict University research. We strongly recommend that this definition be revised to include “software.”

Questions and Answers- Technology and Software Subject to the EAR

We urge BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. Removal from the EAR creates uncertainty created by changes due to interpretive difference. We are concerned that removal of the questions and answers, which we rely upon to guide export control decisions, would create increased uncertainty in our application of key concepts including fundamental research, publication, and educational instruction.

Effective Date of the Final Rule

We requests, at minimum, a six (6) month delay in effective date and further requests that the revised regulations be applicable only to new sponsored research begun after the effective date of the Final Rule.

We appreciate the opportunity to provide comments on these proposed changes.

Sincerely,



James Ashton-Miller
Associate Vice President for Research, Research Policy and Compliance



Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

ATTN: RIN 0694–AG32

RE: BIS Proposed Rule Regarding Revisions to Definitions in the Export
Administration Regulations (BIS–2015–0019)

Via email: publiccomments@bis.doc.gov

Dear Ms. Hess,

SABIC Innovative Plastics US LLC welcomes the opportunity to comment on the proposed rule issued by the Department of Commerce, Bureau of Industry and Security (“BIS”) on June 3, 2015 to revise definitions in the Export Administration Regulations (“EAR”).

SABIC’s Innovative Plastics business unit is headquartered in Pittsfield, Massachusetts and maintains operations in over 35 countries. The company is a global supplier of plastic pellets, sheets, and films that are widely used by its customers to manufacture various articles of commerce in the automotive, healthcare, consumer electronics, transportation, performance packaging, building and construction, telecommunications, and optical media industries. SABIC is committed to abiding by the EAR and ensuring its global operations are compliant with international trade regulations in all jurisdictions.

SABIC greatly appreciates efforts by BIS to improve and streamline the EAR. The proposed rule carves out certain encrypted technology transfers from the definition of “export,” which would facilitate storage and transmission of controlled technology among personnel that are legally authorized. The following comments describe this positive impact in more detail, and also recommend further changes that would enable additional, low-risk transfers to take place more easily, mitigating licensing burdens on BIS and on industry.

Alternative Encryption Standard

Proposed new § 734.18(a)(4)(iii) would allow companies to use encryption that complies with the National Institute of Standards and Technology’s FIPS 140-2 standard or, as an alternative, use “other similarly effective cryptographic means[.]” By contrast, the companion rule proposed by the Department of State, Directorate of Defense Trade Controls (“DDTC”) does not provide this alternative, requiring all encryption to adhere to the FIPS 140-2 standard. SABIC prefers the approach contained in the BIS version because it affords U.S. businesses flexibility in complying

Andrew Dean
SABIC
1310 G. St. NW
Suite 770
Washington, D.C. 20005 US
T: +1 202 621 2552
M: +1 202 257 3621
E: andrew.dean@sabic.com
www.sabic.com

with the proposed regulation. Our company is familiar with the FIPS 140-2 encryption standard and similar alternatives, and we do not anticipate a significant economic impact from implementing such standards for export-controlled transfers. However, our information technology personnel choose from a range of cryptographic options for each specific business need that is presented. This flexibility is essential for the company to maintain control over its business costs. Therefore, we favor the inclusion of alternative cryptographic options.

Email

In recent years, SABIC has migrated many global servers – including its email exchange servers – to an overseas location in order to consolidate business operations. As a result, emails sent by all U.S. employees are “exported” before reaching their intended recipient. If a U.S. person emails export-controlled technology to another authorized U.S. employee with the appropriate encryption in place, under proposed new § 734.18(a)(4) the transfer would not be an export and no licensing would be required. This development represents a welcome shift for SABIC, given that licenses would only be required to authorize recipients but not pass-through server locations. Currently, we advise all employees not to transfer export-controlled technology via email, which impedes their ability to communicate quickly with each other. We offer alternative, less efficient mechanisms for electronic transfers, which require additional resources to manage. The proposed rule would have a positive economic impact by improving communications efficiencies and reducing resource costs.

Enterprise Content Management

The proposed rule enhances our ability to consolidate company data on fewer servers. SABIC is in the process of shifting to a global enterprise content management (“ECM”) system, for which the servers will reside overseas. Licenses would no longer be required to store controlled technology in encrypted documents on ECM servers, provided the system is compliant with § 734.18(a)(4)(iii), as this would no longer be an export. SABIC would not require licenses to permit storage of U.S.-controlled documents on these servers, which facilitates our goal of consolidating company data on the ECM servers. Avoiding the cost of redundant servers in multiple locations is a significant economic benefit to the company.

Third Parties

Occasionally we transfer export-controlled technology to legally authorized third parties in the U.S., such as customers or vendors, who do not have access to SABIC systems. Due to the overseas location of our email exchange servers, we exchange controlled technology by sending physical media via courier in order to avoid licensing burdens. Under proposed new § 734.18(a)(4), U.S. industry could lower costs and improve efficiencies by utilizing secure encrypted email transfers.

Intra-Company Transfers

SABIC recommends that BIS consider creating a new rule or augmenting the current proposed rule to include a licensing exception for intra-company transfers, including deemed exports. Although proposed new § 734.18(a)(4) relieves some of the burden of obtaining licenses for a segment of our typical transfers, inclusion of an intra-company exception would have a far

greater economic impact. Due to SABIC's global operations, we employ domestic and expatriate scientists, engineers, and technologists at research facilities in multiple locations. Their ability to collaborate on export-controlled projects is restricted, requiring the company to apply for standard and deemed export licenses.

SABIC's robust compliance procedures include assessing employee location and citizenship in order to determine eligibility to work on specific export-controlled projects. Implementing an intra-company license exception would accelerate resource allocation flexibility for SABIC and similarly compliant U.S. companies. Without an exception for intra-company transfers, including deemed exports, companies with global operations cannot fully take advantage of proposed new § 734.18(a)(4).

Encourage Other Jurisdictions to Implement Similar Rule

Finally, SABIC recommends that BIS encourage adoption of standards similar to proposed new § 734.18(a)(4) by its partners in multilateral export control regimes. The utility of this proposed rule increases when other countries treat encrypted data transfers and storage similarly. For controlled technology originating at our overseas locations, transfers to authorized recipients could occur without licensing for third-country encrypted storage locations. Similar treatment of encrypted data transfers and storage by other countries would have a positive impact on SABIC as well as others in U.S. industry.

Conclusion

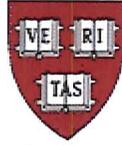
While we are looking forward to the benefits of the proposed rule, we recommend that BIS take additional steps to enhance its overall impact: (1) implement a licensing exception for intra-company transfers, including deemed exports, and (2) encourage multilateral partners to adopt similar regulations that allow for encrypted data transfers and storage.

Thank you for the opportunity to provide comments on the proposed rule to amend the EAR. We welcome the opportunity to further discuss our comments and recommendations with the Department of Commerce, and look forward to working with your agency on other export control reform initiatives.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew Dean".

Andrew Dean
Sr. Manager, Technology Trade Compliance
SABIC



Harvard University
Office of the Vice Provost for Research

Ara Tahmassian
University Chief Research Compliance Officer
ara_tahmassian@harvard.edu
vpr.harvard.edu

Richard A. and Susan F. Smith Campus Center
1350 Massachusetts Avenue, 836
Cambridge, MA 02138
t. 617.495.9797 f. 617.495.8051

Hillary Hess, Director
Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230
Subject: RIN 0694-AG32

Dear Director Hess:

Thank you for allowing us the opportunity to comment on the Commerce Bureau of Industry and Security (“BIS”) and the State Department Directorate of Defense Trade Controls (“DDTC”) sets of proposed revisions intended to harmonize definitions in the Export Administration Regulations (“EAR”) and International Traffic in Arms Regulations (“ITAR”). We greatly appreciate the opportunity to comment on these proposed revisions, as they impact the conduct of research and collaboration at the heart of our educational mission.

Harvard University takes very seriously its responsibilities under the export control laws. The University has a policy concerning compliance with these rules; has an export council comprised of individuals across the University’s thirteen schools and chaired by myself as the Chief Compliance Officer; and has used written materials, general training sessions, and targeted training to remind faculty, researchers, and administrators of applicable existing and emerging export control requirements. The release of the proposed amendments, while intended “to reduce unnecessary regulatory burdens,” has raised a number of concerns within the academic scientific community. Institutions of higher education play a vital role in our economic and physical security. We trust that the government is committed to working with the academic and research community to ensure that our nation’s export control policies do not undermine the openness and strength of universities like Harvard.

Although we agree with the comments proffered by COGR, AAU and APLU, we write separately to emphasize three areas of particular concern in response to the issues on which BIS and DDTC have requested specific comments and urge BIS to revise the definitions further to address these concerns:

1. The scope of the fundamental research exclusion;
2. The scope of the educational exclusion; and
3. The proposed removal of the Q & As from the Federal Register.

We discuss each of these in turn below.

1. Fundamental Research.

We appreciate the clarification that technology that either “arises during” or “results from” fundamental research and is “intended to be published” is not subject to EAR. We are concerned, however, that you have inadvertently narrowed the scope of the fundamental research exclusion, while simultaneously proposed eliminating essential guidance in the the Q&As found in Supplement No. 1. Official government policy on the transfer of scientific and technical information as reflected in National Security Decision Directive (NSDD) 189 states that “No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.” Conduct of fundamental research may draw upon a wide range of information and other inputs. In drawing a sharp distinction between the conduct and results of fundamental research, BIS appears to be arbitrarily restricting NSDD-189 without clear authority.

First, foreign researchers, who have, with government approval, secured visas to study here, might, in the conduct of their research, have access to controlled equipment and technology. There are approximately 2,000 laboratories at Harvard, disbursed throughout undergraduate and graduate programs in two cities. Equipment and technologies that appear on the controlled list would be found in a large percentage of these laboratories. In addition, Harvard has thousands of active students who are neither U.S. citizens nor U.S. permanent residents, and foreign scholars with Harvard appointments at both the University and its affiliated hospitals. These international students and scholars study, teach, and participate in open research projects and, importantly in an academic setting, interact in a free environment across our campuses.

In the past, Harvard did not apply for a deemed export license when foreign scholars had access to such technology under the EAR because our researchers did not engage in the “use” of the technology, as defined by the government. In order for technology to be considered “use,” it had to include six elements: operating, installing, maintaining, repairing, overhauling, and refurbishing. In the ordinary course, researchers would operate or even repair a controlled item, but they would not generally maintain, overhaul, or refurbish the equipment. Thus, the operation of such equipment was not “use” technology as defined by the EAR.

Second, Note 1 to revised Section 734.8, in our view, is too broad. It not only sweeps in certain use technology that was previously excluded but also risks the inclusion of standard, off-the-shelf technology and software that did not arise during or result from fundamental research.

We would urge the government to make clear that access to controlled equipment, software, or technology in the conduct of open research for those properly authorized to study and work here does not trigger a licensing requirement. *Restricting the use of widely used and commercially available technology or of controlled equipment in the conduct of fundamental research would have the practical effect of restricting or limiting the research itself.*

Unlike commercial proprietary research, research in a university setting has few boundaries. Once students and scholars are permitted by the government to enter this country on valid visas, the U.S. will gain the greatest benefit from fundamental research conducted by these individuals if their research remains free and open, including for access to technology directly associated with such research. Indeed, it is this diversity and fluidity that have resulted in our greatest scientific advancements – advancements that are open for broad dissemination and scrutiny.

We note further that the ITAR changes in the note to Part 120.49(a) specifically states that access to controlled technology under fundamental research could itself be controlled. (“The inputs used to conduct fundamental research, such as information, equipment or software, are not ‘technical data that arises during or results from fundamental research’ except to the extent that such inputs are technical data that arise during or result from earlier fundamental research.”)

We fully understand the national security implications of conducting fundamental research in technologies subject to the ITAR and the importance of a careful review of access to such technologies. Nevertheless, if the State Department has determined through regulation that certain research should be eligible for fundamental research, we believe the exclusion should apply.

The addition of the note would effectively swallow the fundamental research determination as access to commercially available equipment and software controlled under the ITAR frequently would be necessary to conduct fundamental research under the ITAR. The inclusion of this note would dramatically inhibit the ability to conduct fundamental research that would otherwise qualify for Part 120.49. Quite simply, some research, which would otherwise qualify as fundamental research, would be ineligible for the exclusion because of the need to access ITAR-controlled equipment or software to conduct the research. To the extent the note is retained, we recommend removing the terms “equipment” and “software.”

2. Educational Exclusion.

The new provision regarding educational information subject to the EAR imports language from ITAR regarding “general scientific, mathematical, or engineering principles” and dramatically circumscribes the scope of the educational exclusion. While we understand the need for, and desire to, harmonize language across regulatory regimes, in this instance, the effort to harmonize has resulted in a gross departure from the original scope of this provision in the EAR.

The current language in the EAR excluding educational information from the scope of the EAR states that educational information “is not subject to EAR if it is released by instruction in catalog courses and associated teaching laboratories of academic institutions.” If a course is publicly advertised in a course catalog, then it is not subject to EAR. We have two concerns with the insertion of the additional requirement that the exclusion only applies to “general scientific, mathematical, or engineering principles.”

First, the new language suggests that a research institution like Harvard would have to make subtle judgments about which courses would be eligible for the exclusion and which would not. This is a virtually impossible task.

Second and related, the term “general” is susceptible to wide swings in interpretation. An upper-level course in computers for a graduate student may be a general requirement for the degree. Is a basic mathematical programming course that introduces students to the fundamentals of mathematical programming a “general” course eligible for the exclusion? While it may be appropriate under ITAR to limit access to the most sensitive technologies, it is not appropriate for the EAR regulatory regime.

From the language in the proposed notice, it does not seem to be the intent of these revisions to expand the scope of the EAR. The proposed notice explicitly states that the revised language regarding what educational information is considered to be outside the purview of the EAR is “not intended to make a change to the scope of the current section.” In view of this, we respectfully suggest adding: “/or” to this provision, so that it reads:

“Concern general scientific, mathematical, or engineering principles commonly taught in schools, **and/or** released by instruction in a catalog course or associated teaching laboratory of an academic institution;”

3. The Inclusion of the Q&As in the Federal Register.

While we appreciate that Q&As are often considered illustrative, the Q&As in Supplement No. 1 convey important regulatory information that has been previously conferred considerable weight. When navigating the application of export controls requirements to university communities, which are large, diverse, and complex, the Q&As have provided clear and useful guidance not only to educational institutions but also to government agencies regarding the types and nature of activities of concern. Below are examples of questions and answers that have been useful to diverse research and educational institutions like Harvard:

Question C(1): I teach a university graduate course on design and manufacture of very high-speed integrated circuitry. Many of the students are foreigners. Do I need a license to teach this course?

Answer: No. Release of information by instruction in catalog courses and associated teaching laboratories of academic institutions is not subject to the EAR (§734.9 of this part).

Question C(2): Would it make any difference if some of the students were from countries to which export licenses are required?

Answer: No.

Question C(3): Would it make any difference if I talk about recent and as yet unpublished results from my laboratory research?

Answer: No.

Question C(4): Even if that research is funded by the Government?

Answer: Even then, but you would not be released from any separate obligations you have accepted in your grant or contract.

Question D(1): Do I need a license in order for a foreign graduate student to work in my laboratory?

Answer: Not if the research on which the foreign student is working qualifies as “fundamental research” under §734.8 of this part. In that case, the research is not subject to the EAR.

Question D(2): Our company has entered into a cooperative research arrangement with a research group at a university. One of the researchers in that group is a PRC national. We would like to share some of our proprietary information with the university research group. We have no way of guaranteeing that this information will not get into the hands of the PRC scientist. Do we need to obtain a license to protect against that possibility?

Answer: No. The EAR do not cover the disclosure of information to any scientists, engineers, or students at a U.S. university in the course of industry-university research collaboration under specific arrangements between the firm and the university, provided these arrangements do not permit the sponsor to withhold from publication any of the information that he provides to the researchers. However, if your company and the researchers have agreed to a prohibition on publication, then you must obtain a license or qualify for a License Exception before transferring the information to the university. It is important that you as the corporate sponsor and the university get together to discuss whether foreign nationals will have access to the information, so that you may obtain any necessary authorization prior to transferring the information to the research team.

Question D(3): My university will host a prominent scientist from the PRC who is an expert on research in engineered ceramics and composite materials. Do I require a license before telling our visitor about my latest, as yet unpublished, research results in those fields?

Answer: Probably not. If you performed your research at the university, and you were subject to no contract controls on release of the research, your research would qualify as “fundamental research” (§734.8(a) of this part). Information arising during or resulting from such research is not subject to the EAR (§734.3(b)(3) of this part).

You should probably assume, however, that your visitor will be debriefed later about anything of potential military value he learns from you. If you are concerned that giving such information to him, even though permitted, could jeopardize U.S. security interests, the Commerce Department can put you in touch with appropriate Government scientists who can advise you. Send written communications, via courier, to: Department of Commerce, Bureau of Industry and Security, Room 2099B, 14th Street and Pennsylvania Ave., NW., Washington, DC 20230.

Question D(4): Would it make any difference if I were proposing to talk with a PRC expert in China?

Answer: No, if the information in question arose during or resulted from the same “fundamental research.”

Question D(5): Could I properly do some work with him in his research laboratory inside China?

Answer: Application abroad of personal knowledge or technical experience acquired in the United States constitutes an export of that knowledge and experience, and such an export may be subject to the EAR. If any of the knowledge or experience you export in this way requires a license under the EAR, you must obtain such a license or qualify for a License Exception.

Question D(6): I would like to correspond and share research results with an Iranian expert in my field, which deals with technology that requires a license to all destinations except Canada. Do I need a license to do so?

Answer: Not as long as we are still talking about information that arose during or resulted from research that qualifies as “fundamental” under the rules spelled out in §734.8(a) of this part.

Question D(7): Suppose the research in question were funded by a corporate sponsor and I had agreed to prepublication review of any paper arising from the research?

Answer: Whether your research would still qualify as “fundamental” would depend on the nature and purpose of the prepublication review. If the review is intended solely to ensure that your publications will neither compromise patent rights nor inadvertently divulge proprietary information that the sponsor has furnished to you, the research could still qualify as “fundamental.” But if the sponsor will consider as part of its prepublication review whether it wants to hold your new research results as trade secrets or otherwise proprietary information (even if your voluntary cooperation would be needed for it to do so), your research would no longer qualify as “fundamental.” As used in these regulations it is the actual and intended openness of research results that primarily determines whether the research counts as “fundamental” and so is not subject to the EAR.

Question D(8): In determining whether research is thus open and therefore counts as “fundamental,” does it matter where or in what sort of institution the research is performed?

Answer: In principle, no. “Fundamental research” is performed in industry, Federal laboratories, or other types of institutions, as well as in universities. The regulations introduce some operational presumptions and procedures that can be used both by those subject to the regulations and by those who administer them to determine with some precision whether a particular research activity is

covered. Recognizing that common and predictable norms operate in different types of institutions, the regulations use the institutional locus of the research as a starting point for these presumptions and procedures. Nonetheless, it remains the type of research, and particularly the intent and freedom to publish, that identifies “fundamental research,” not the institutional locus (§734.8(a) of this part).

Question D(9): I am doing research on high-powered lasers in the central basic-research laboratory of an industrial corporation. I am required to submit the results of my research for prepublication review before I can publish them or otherwise make them public. I would like to compare research results with a scientific colleague from Vietnam and discuss the results of the research with her when she visits the United States. Do I need a license to do so?

Answer: You probably do need a license (§734.8(d) of this part). However, if the only restriction on your publishing any of that information is a prepublication review solely to ensure that publication would compromise no patent rights or proprietary information provided by the company to the researcher your research may be considered “fundamental research,” in which case you may be able to share information because it is not subject to the EAR. Note that the information will be subject to the EAR if the prepublication review is intended to withhold the results of the research from publication.

Question D(10): Suppose I have already cleared my company's review process and am free to publish all the information I intend to share with my colleague, though I have not yet published?

Answer: If the clearance from your company means that you are free to make all the information publicly available without restriction or delay, the information is not subject to the EAR. (§734.8(d) of this part)

Question D(11): I work as a researcher at a Government-owned, contractor-operated research center. May I share the results of my unpublished research with foreign nationals without concern for export controls under the EAR?

Answer: That is up to the sponsoring agency and the center's management. If your research is designated “fundamental research” within any appropriate system devised by them to control release of information by scientists and engineers at the center, it will be treated as such by the Commerce Department, and the research will not be subject to the EAR. Otherwise, you would need to obtain a license or qualify for a License Exception, except to publish or otherwise make the information public (§734.8(c) of this part).

* * *

Such guidance, with the force that accompanies notice in the Federal Register including comment periods such as BIS and DDTC are undertaking for this exercise, is necessary to ensure scrupulous compliance. We, therefore, respectfully request that that the Q&As remain in the EAR.

Harvard is committed to working with the government to establish policies, rules, and regulations that both protect the nation's security and ensure scientific, technological, and economic advancements. We hope you will further clarify the appropriate scope of the fundamental research and education exclusions and include the helpful questions and answers in Supplement 1, consistent with our comments.

Sincerely,

A handwritten signature in blue ink that reads "A. Tahmassian". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Ara Tahmassian
University Chief Research Compliance Officer



August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

Subject: RIN 0694-AG32 (Proposed new definitions to the EAR)

Dear Ms. Hess:

On behalf of The Ohio State University (OSU), I am pleased to provide our response to your request for comments on the proposed Revisions to Definitions in the Export Administration Regulations (EAR).

As a thriving \$983M research enterprise, OSU takes seriously its responsibilities for effective stewardship of the federal and private-sector funds that support our many research and training activities. While we appreciate the federal government's need to ensure that taxpayer funds are used effectively, we are also acutely aware of the burden that the ever-increasing set of compliance requirements is creating for higher education institutions. Managing the complexities of often-conflicting requirements detracts from productive research time for our investigators and leads to significant delays in the onset and conduct of research projects.

In putting forth the proposed EAR definitions, we believe it was the Department of Commerce's intent to clarify existing rules and harmonize the structure of the rules to align with the ITAR. We applaud this initiative and believe that in many ways the effort has been successful. However, there are several areas where seemingly small changes in the rules could have a significant and deleterious effect on university-based research in the United States.

As a member of COGR, AAU, and APLU (the associations), OSU concurs with the thoughtful and detailed responses these organizations are providing to BIS's request for comment. We will focus here on two topics that are of particular interest and concern to OSU and its research enterprise.

I. Educational Information

One change that could have a marked impact on educational institutions is the restatement of the 'education exemption.' The new EAR language has been combined with ITAR 120.10(b) and now states that "information and software that ...concern general scientific, mathematical, or engineering principles *commonly taught in schools*, and released by instruction in a catalog course or associated

teaching laboratory of an academic institution" are not subject to EAR. See 15 C.F.R. § 734.3(b)(3)(iii) (proposed)(emphasis added). The "*commonly taught in schools*" language is new and potentially problematic because some university courses, particularly capstone-type courses, include novel information and/or present cutting-edge research. Furthermore, many catalog courses include hands-on laboratories that will necessarily differ by institution, professor, and class participation. Under a narrow interpretation of the proposed rule, these types of courses would not fall under the education exclusion, and any unpublished material presented would be subject to export rules. As education at universities is intended to be open, and limited only by course prerequisites, this new rule could significantly hinder the ability of U.S. institutions to develop instruction in emerging areas.

OSU would prefer that the current definition of educational information be retained. See 15 C.F.R. § 734.9 (eff. Jan. 7, 2011). However, we also support the associations' proposal that the definition be modified to read "information and software that concern general scientific, mathematical, or engineering principles commonly taught in schools and/or released by instruction in a catalog course or associated teaching laboratory of an academic institution."

II. "Fundamental Research", "Technology", and "Software"

While the definition of Fundamental Research does not appear to have been modified significantly, we strongly support retaining the current definition—15 C.F.R. § 734.8 (eff. Jan. 7, 2011)—which has been endorsed by White House Administrations of both parties over the years and has served the scientific community well.

There is, however, one significant change that causes potential concern. Section 734.3(b)(3) of the current rules states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. The proposed § 734.8(a) states: "'Technology' that arises during, or results from, fundamental research and is 'intended to be published' is . . . not be subject to the EAR." However, there is also a preamble reference to a proposed note "to clarify that software and commodities are not 'technology resulting from fundamental research.'" 80 Fed. Reg. 31,505, 31,507 (Jun. 3, 2015). We interpret this reference to mean that software (source code) which results from fundamental research would be subject to deemed export restrictions, even if the software is intended to be publicly available, while a natural-language document describing that source code would be considered fundamental research. Because there is no obvious or stated rationale for this distinction, we recommend revising the proposed rule to read: "'technology' or 'software' that arises during, or results from, fundamental research and is 'intended to be published' is thus not 'subject to the EAR.'"

III. Conclusion

In summary, we believe that the proposed rules incorporate many helpful changes and clarifications that go a long way towards harmonizing the EAR with the ITAR. However, we are very concerned that the unintended narrowing of the Educational Information exclusion and the removal of "software" from the Fundamental Research exclusion would have significant ramifications for U.S. institutions of higher education and could have a chilling effect on United States research as a whole.

Thank you for your consideration of our input. Should you have questions or require more information, please contact me.

Sincerely,

A handwritten signature in black ink that reads "Caroline Whitacre". The script is cursive and fluid, with the first name "Caroline" and last name "Whitacre" clearly legible.

Caroline C. Whitacre, Ph.D.
Vice President for Research
Professor of Microbial Infection and Immunity



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0026

Tracking Number: 1jz-8kck-5gsg

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Clint Davis

Comment

I oppose the proposed arms control regulations



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed

Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0027

Tracking Number: 1jz-8kck-dcxb

Document Information

Date Posted:

Aug 4, 2015

RIN:

0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:

Shaun Anonymous

Comment

To whom it may concern:

I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State Department a wide-ranging power to monitor and control gun-related speech on the Internet.

The new language -- which includes making technical data available via a publicly available network (e.g., the Internet) -- could put anyone who violates this provision in danger of facing decades in prison and massive fines.

So posting information on virtually any firearm or ammunition could be defined by the Obama administration as requiring, not only government permission, but potentially a government license. This means violators would potentially face significant criminal penalties.

I also oppose the addition of the word software into these regulations, as it appears to be a not-so-veiled effort to ban 3-D printers.

I urge you to repeal these new regulations in their entirety. Whether you like it or not, the First and Second Amendments are still the law of the land!

Sincerely,
Shaun



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0028

Tracking Number: 1jz-8kck-pni0

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Sam Schieuer

Comment

Any attempt to regulate free speech about firearms on the internet is nothing but an attempt to demolish the first AND second amendment rights. Your duty as the govt is to uphold our rights, not take them away. Very AGAINST this.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0029

Tracking Number: 1jz-8kck-58m2

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Thaddeus Warner

Comment

To whom it may concern:

I strongly oppose the rewrite of the State Departments arms control regulations (ITAR), which could potentially grant the State Department a wide-ranging power to monitor and control gun-related speech on the Internet.

The new language -- which includes making technical data available via a publicly available network (e.g., the Internet) -- could put anyone who violates this provision in danger of facing decades in prison and massive fines.

So posting information on virtually any firearm or ammunition could be defined by the Obama administration as requiring, not only government permission, but potentially a government license. This means violators would potentially face significant criminal penalties.

I also oppose the addition of the word software into these regulations, as it appears to be a not-so-veiled effort to ban 3-D printers.

This proposal is 100% unconstitutional and will serve to anger many people. I, and many others, are prepared to donate our time and money to support litigation against the state department should such a thing occur.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0030

Tracking Number: 1jz-8kck-zgbe

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Thomas Brewer

Comment

This rule should be rejected outright, as it is simply an attempt at government control of the internet, using information that

exists in the open market in any bookstore or library in America as a strawman. It also is a violation of the First Amendment

in regards to free speech.



August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C. 20037

Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C. 20230

Regulation IDs: RIN 1400-AD70 and RIN 0694-AG32

Dear Mr. Peartree and Ms. Hess,

The Aerospace Industries Association (AIA) and our member companies welcome the opportunity to provide comment in response to the Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), (80 Fed. Reg. 31, 525 and 80 Fed. Reg. 31, 505). AIA continues to support the President's Export Control Reform Initiative (ECR) and views the harmonization of definitions across the ITAR and EAR a critical step in the ECR process, encouraging consistency of classification and application.

Comments on Proposed Revisions to Definitions in the ITAR and EAR

§ 120.6 Defense Article.

1. AIA supports the changes to the definition of Defense Article and the removal of software to further align with the EAR. In our review, we recognized a potential oversight to the proposed changes to § 120.6(a). It is understood that * * * means the remaining paragraph language of (a) remains intact, to include the original exclusion language "*It does not include basic marketing information on function or purpose or general system descriptions.*" AIA recommends this language be removed from § 120.6(a) as it will be captured in the revised definition of technical data.

§ 120.10 Technical data, § 772 Technology

1. The proposed language at § 120.10(a)(1) includes *installation* in the definition of technical data. In comparing the Note to Paragraph (a)(2) of 120.9, it would appear that the act of installation is one that does not require technical data. If installation does not require technical data, then it would appear to be contradictory to include the term *installation* in the definition of technical

data. AIA recommends the removal of the term *installation* in the definition of technical data. To establish consistency, AIA additionally recommends the removal of the term *installation* in the definition of technology.

2. We recommend the removal of the phrase “...or information gleaned through visual inspection;” from paragraph (a)(1) as it relates to a form or method in which technical data may be transferred, i.e. “exported”, rather than what information constitutes technical data.
3. We do not agree with the addition of (a)(5) in the definition of technical data and technology. Decryption keys, network access codes and passwords are not in and of themselves export controlled items. AIA understands the goal with this change is to capture the event of a foreign person accessing encrypted controlled information, and as such AIA recommends that DDTC and BIS consider moving the language in (a)(5) to the definition of Release at and create a new section:

(a)(3) Accessing encrypted technical data by applying a decryption key, network access code or password.

Fundamentally, if decryption keys, network access codes and passwords were technical data, sending a decryption key, network access code or password to the wrong non-U.S. person would be considered an export violation, even if possession of the key, code or password was incapable of being used. For example, if Mr. John Smith, a non-U.S. person, received encrypted information, but the key, code or password was sent to different John Smith that was not in the same location or even same company as the recipient of the encrypted information, the wrong John Smith could not use the key, code or password and possession would be meaningless.

Additional rationale for removing decryption keys, network access codes and passwords from the definition is if an export controlled document is encrypted and emailed, the password could be a simple phrase to open the document (e.g., exporting is fun). This password, by way of this definition, is now export controlled and must be treated appropriately meaning all instances where this phrase appears instantly becomes export controlled. Taking this argument to another level, all derivative usage of the password phrase is also export controlled. Industry is ill-equipped to manage such an overreaching application of controls to passwords.

Finally, AIA could not readily identify which USML category or ECCN would capture the controls of passwords and decryption keys. Their absence from the USML and CCL supports the argument that the event of accessing the data is what DDTC and BIS are trying to control rather than the passwords and decryption keys themselves.

4. We recommend the removal of the term “non-proprietary” from the term “~~non-proprietary~~ general system descriptions;” as whether data is proprietary does not indicate whether something is technical data or not. Many proposals are proprietary (e.g., for commercial reasons) and contain general system descriptions. Companies make business decisions to describe certain systems descriptions as “proprietary” for various reasons. It would unnecessarily serve as a “chilling effect” on companies if they were aware the mere act of describing a description as proprietary would make it technical data. Further, including this wording is an increase in control. The number of licenses would increase exponentially as a result of controlling propriety data, which would significantly impact license processing times. This would be inconsistent with one of the goals of ECR to limit export control over those

articles or information most important to the national security and foreign policy interests of the United States.

5. We note that DDTC has specifically called out “Telemetry data” in 120.10(b)(3) as not being Technical Data, yet AIA believes this is already established by Note 3 to Paragraph (f) to USML Category XV (Spacecraft). If it is nonetheless the intention of DDTC to specifically identify telemetry data in 120.10(b), then AIA recommends adding a new subparagraph 120.10(b)(4) that would also specifically identify that “activities and technology and other information directly related to or required for the spaceflight passenger or participant experience” as described in Note 2 to paragraph (f) of USML Category XV are also not “technical data.”

That said, there could be other instances driven by notes to USML Categories where data has been or will be specifically excluded from the definition of “technical data” so the more appropriate solution may be to simply remove sub-paragraph (b)(3) to 120.10, or amend its text to state “any technical data or other such information that is specifically identified within the USML, including notes thereto, as not being subject to the ITAR.”

§ 120.17 Export, § 734.13 Export

1. AIA requests the removal of (a)(6) from the definitions of Export as our recommendation is to move this requirement to the definition of Release (see above reference) and to amend the proposed § 120.17(a)(1) and § 734.13(a)(1) to

“(a)(1) An actual shipment, *release*, or transmission out of the United States,”

AIA would like to emphasize its concern with the language utilized in the proposed definition ‘*providing physical access that would allow access to other technical data*’. This language is quite broad and could be interpreted to mean that physical access to a room where technical data happens to reside and is not intended to be transferred to the foreign person would be considered an export. AIA believes that the measures industry takes to physically control technical data on their premises in order to comply with the ITAR, EAR and NISPOM, as well as company policies on securing company data, are sufficient to ensure that controlled information is not arbitrarily provided to a foreign person. The removal of (a)(6) addresses this concern.

2. The proposed definition of “export” adds paragraph (b) which explicitly states that release of “technical data” to a foreign person is deemed to be an “export” to all countries in which the foreign person has held citizenship or holds permanent residency. As between the ITAR and the EAR there are two standards, namely one that includes, “all previous citizenships” versus only country of last citizenship obtained. Maintaining two different standards increases the regulatory burden on U.S. exporters and is inconsistent with the goal of Export Control Reform to harmonize the two sets of regulations.

We recommend that the § 120.17 be modified to remove, “. . . and all countries in which the foreign person has held citizenship” to read as follows:

“Any release in the United States of technical data or software to a foreign person is a deemed export to ~~all countries in which the foreign person has held citizenship~~ the foreign person’s most recent country of citizenship or permanent residency.”

§ 120.19 Reexport, § 734.14 Rexport

AIA requests the removal of (a)(4) from the definitions of Reexport as our recommendation is to move this requirement to the definition of Release (see above reference) and to amend the proposed § 120.19(a)(1) and §734.14(a)(1) respectively to:

“(a)(1) An actual shipment, *release*, or transmission of a defense article...”

“(a)(1) An actual shipment, *release*, or transmission of an item...”

§ 120.46 Required

We recommend including in Note 3 to paragraph (a) the following example for illustrative purposes:

Note 3 to paragraph (a): An illustration of determining whether technical data” is ‘peculiarly responsible’ for achieving or exceeding controlled performance levels, characteristics, or functions’ is as follows: Assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are *not peculiarly responsible* for producing the controlled product “X”. However, if technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” *were peculiarly responsible* for making the controlled product and are themselves “required” and therefore controlled as “technical data.”

§120.47 Development

The last sentence in this section of the proposed rule states, “*Development includes modification of the design of an existing item.*”

This statement is overly broad and AIA recommends rewriting it as follows: “*Development includes modification of the design of an existing item only when it alters the function or performance capabilities. It does not include modifications of items with equivalent form and fit.*” Additionally this aligns with the EAR definition of development.

§ 120.49 Technical data that arises during, or results from, fundamental research.

AIA believes the word ‘located’ has been extraneously added to the end of § 120.49(a)(1) and suggest it be deleted.

§ 120.52 Activities that are not exports, reexports, or retransfers, § 734.18

1. It was noted in the proposed subparagraph (b) that the term ‘given’ was utilized rather than ‘released’. AIA recommends the following edits: “... where the means to access the data in unencrypted form is not *released* to any third party”

2. Level of security: The rule states, “Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors...” We recommend that the rule specify the modules must be compliant with FIPS 140-2, Level 1. FIPS 140-2 acknowledges four levels of security, and since the data in question is unclassified it should be subject to Level 1.
3. Scope of NIST publications: “Guidance provided in current U.S. National Institute for Standards and Technology publications” could be interpreted to have nearly an unlimited scope due to the large volume of relevant NIST publications. The rule should cite NIST Special Publication SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* as the reference standard for this clause. The controls selected from SP 800-53 should not exceed those in Table 1 of DFARS 252.204-7012, *Safeguarding of Unclassified Controlled Technical Information*.
4. Revision implementation: As written, each time NIST published a revision would cause IT systems to export until they are brought into compliance with the new revision. The rule should allow compliance with the prior NIST revision for one year beyond the publication date.
5. The proposed rule states: “(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; and (4) Sending, taking, or storing technical data or software that is...”

We recommend that the word “and” be changed to “or” to clarify these activities are not conjunctive.

§ 120.9 Defense Services

1. Coordination with 80 FR 30001 (Note 1 to paragraph (a)(1)): The proposed rules in 80 FR 31505 and 80 FR 30001 deal with the same subject and should be published with the same effective date.
2. Use of knowledge of technical data to determine whether a defense service has been provided. AIA members are deeply concerned about the attempt to define defense services based on the “knowledge” of relevant technical data by an involved US person. It is highly problematic to base this standard based on what an engineering resource may have contained in his/her brain. This could set up truly difficult enforcement cases that do not hinge on what was actually provided to the non-US entity that received the service but the knowledge of the engineer or service technician involved in providing the service. AIA submits the knowledge of the individual involved should not be dispositive in determining whether a “defense service” has been provided, but rather the rules must focus on what benefits the non-US entity received related to the defense article(s).
3. Scope of USML Paragraph (Note 1 to paragraph (a)(1) of proposed 120.9): The language “in the same USML paragraph or accessed” is excessively broad because USML paragraphs are themselves very broad and thus impute to U.S. persons “knowledge” of technical data where

none exists. For example, in Category XI—Military Electronics, paragraph “(a)” includes both “[a]ctive or passive acoustic array sensing systems” and “[r]adar systems and equipment,” two largely different disciplines of engineering. As a consequence, potentially many more U.S. persons would fall under this clause than envisioned by DDTTC. We recommend instead using “the same USML paragraph subsection.”

4. Country of Origin for Programs and Technical Data (Note 1 to paragraph (a)(1) of proposed 120.9): If knowledge is to be imputed, the rule should be particular to U.S. development activity and U.S.-origin technical data. It is unreasonable to control as a defense service under the ITAR the activities of a natural person born in a foreign country and currently working for a foreign employer in that country and only having defense program experience in that country, simply because the natural person acquired U.S. person status.
5. Note to paragraph (a)(1) includes, “...or accessed (physically or electronically) technical data directly related to the defense article that is the subject of the assistance, prior to performing the service.”

We recommend revising or removing this language because (1) the term “access” is too broad as it does not necessarily involve actual access to the technical data, and (2) the language “prior to” does not have any reasonable contemporaneous time reference, meaning it could have been at any past point in a lifetime. As a result, as written, “knowledge of U.S.-origin technical data” could be presumed if, 20 years prior to performing a service, an individual accessed a file containing technical data even though the individual did not study or utilize such data at that time or since.

§ 120.11 Public Domain, § 127.1 Violations

These sections refer in several instances to a general “knowledge” standard. AIA believes that depending on the knowledge standard applied, the text could impose a severe administrative burden on corporate persons. If knowledge is imputed by possession of historical records, persons may be obligated to research historical archives to determine whether or not they had “knowledge” that information made publicly available in the past was unauthorized. The language should be reframed to be forward-looking and apply a strict standard of “knowledge.”

§ 125.4(b)(9) Exemptions of general applicability.

1. AIA believes that this language unnecessarily restricts the exemption use for long-term assignments abroad and the utilization of expatriates living in the foreign country. Many defense contractors have contracts servicing U.S. installations abroad that at the end of the negotiated term are renewed; keeping the employee abroad for a longer period of time. AIA could not readily identify the rationale for limiting the exemption to the amount of time the U.S. employee happens to be abroad. When an employee receives technical data while abroad and returns to the U.S. in two weeks, two years, or twenty years, there is no change to the original export. AIA supports the exemption as it is currently applied, and keeping the proposed language in the exemption will hamper the defense industry’s ability to support long term contracts for the U.S. military performed in foreign locations; most likely resulting in obtaining export licenses that are currently not required and generating a burden to both the government and industry. Therefore, AIA requests that the language be removed and § 125.4(b)(9) be revised as outlined below:

“(b)(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or foreign person employee of a U.S. person is subject to the following restrictions...”

2. The proposed rule paragraph (vi) states, “Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed).”

We request clarification as to whether a party would be at risk of violating the NISPOM if they were to follow the guidance of DDTC.

§ 127.1(b)(4) Violations, § 764.2(l) Violations

AIA requests the removal of § 127.1(b)(4) as our recommendations to amend the proposed definitions of Export at §120.17(a)(1) and Reexport at §120.19(a)(1) would not warrant a change to §127.1 as violations occur when a defense article or technical data is exported or reexported unlawfully as described. We believe § 127.1(a)(1) is sufficient as written and would capture the exposure addressed by the proposed language at § 127.1(b)(4).

Similarly, AIA requests the removal of § 764.2(l) in its entirety as the current language of § 764.2 is adequate.

EAR §§ 734.20 and 750.7 Permanent and Regular Employee

1. AIA’s member companies disagree with the proposed definition and use of the phrase “permanent and regular employee” in §§ 734.20 and 750.7(a) to require employment for 1 year or longer. In practice, the term “permanent and regular employee” generally is applied to contract or contingent workers in foreign facilities. Mandating a period of 1 year or longer for the relationship significantly compromises the ability of a non-US defense company to take advantage of the provisions that use this phrase. Many companies do not employ contract workers for periods of a year or longer because doing so can create a risk under labor and employment law that the contract worker would take legal action to acquire the benefits and other rights of employees.

The five specific criteria enumerated under §734.20(d)(2) are adequate to ensure appropriate control of EAR data in that the worker must: (i) work at the company’s facilities; (ii) work under the company’s direction and control; (iii) work full time and exclusively for the company; (iv) execute nondisclosure certifications for the company and (v) not be taking direction from the staffing company. Why is it necessary for the relationship to be “long term” if those criteria are satisfied? The company engaging the contract employee will be responsible for the conduct of the worker regardless. The company can decide the length of relationship that would be appropriate given these competing considerations.

Moreover, the timing requirement does not necessarily apply or make sense in other contexts. What if a company hires an individual for permanent employment and the employee quits after 30 days? There ultimately would be no “long term” relationship under those circumstances

either, yet it is not clear in the proposed definition and use of the phrase whether the employee would fall under the “permanent and regular” definition after being hired.

AIA also requests further clarification on how the proposed use of the phrase “permanent and regular employee” in § 750.7 may impact existing licenses. BIS typically limits employees authorized to receive controlled data through the inclusion of conditions with the license but does not put a restriction on the amount of time an employee must be working at a facility. If the proposed changes to § 750.7(a) are finalized, what happens to employees under existing licenses that do not meet the specified “permanent and regular employee” definition but were not explicitly limited in the license conditions?

AIA strongly urges BIS to change the proposed language as follows:

§ 734.20 Activities that are not “deemed reexports.”

(b) Release to A:5 nationals...

(1) * * *5 nationals...

(2) The foreign national is a regular ~~and permanent~~ employee...

(c) Release to other than A:5 nationals...

(1) * * *release to other than A:5 nationals.

(2) The foreign national is a regular ~~and permanent~~ employee...

(d) Definitions

(1) * * *

(2) “~~Permanent and~~ is an individual who:

(a) Is ~~permanently (i.e., for not less than a year) and~~ directly employed by an entity, or

(b) Is a contract employee who:

(i) Is in a ~~long term~~ contractual relationship with the company...

§ 750.7(a) ... A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity’s foreign nationals who are ~~permanent and~~ regular employees (and who are not proscribed persons under US law)...

AIA appreciates the opportunity to provide comments and looks forward to continue to work with DDTC and BIS as the U.S. Government addresses additional areas of reform.

Best Regards,



Remy Nathan
Vice President – International Affairs
Aerospace Industries Association



UNIVERSITY of VIRGINIA
Finance Outreach and Compliance

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am writing on behalf of The Rector and Visitors of the University of Virginia (University or University of Virginia) to comment on the proposed Revisions to Definitions in the Export Administration Regulations (EAR) and certain corresponding changes to the International Traffic in Arms Regulations (ITAR). We believe that these revisions, if adopted as proposed, will undermine the University's ability to deliver on our core academic missions of providing high quality research, teaching and service.

Educational Information

Under the EAR "educational information" is currently defined in §734.9 and specifically excluded from the scope of the regulations in §734.3(b)(3)(iii). Both the definition and exclusion are well understood and consistently applied by the Bureau of Industry and Security (BIS) and the academic community. We are concerned that the removal of the definition of "educational information" and the limitation of the exclusion in §734.3(b)(3)(iii) to information and "software" that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution will create uncertainty and raise questions regarding the applicability of the exclusion to new University courses. The University and other institutions of higher education must be able to freely develop new courses to meet the ever changing needs of our students and expectations of prospective employers including, but not limited to, the U.S. Government without having to be concerned with whether or not the content is "general" and "commonly taught." In addition to this concern regarding newly developed courses, many advanced undergraduate and graduate level catalog courses include hands on design laboratories in which students determine their own projects, which may or may not include the production of prototypes. Will the intellectual content of these courses, which would have previously been treated as "educational information," now become subject to the EAR because they go beyond providing instruction on general theories or principles?

The University of Virginia joins with the Association of University Export Control Officers (AUECO) in recommending that the qualifier "concern general scientific, mathematical, or engineering principles commonly taught in schools" be removed and that the simpler "is released by instruction in catalog courses and associated teaching laboratories of academic institutions" be retained for §734.3(b)(3)(iii). We prefer this approach to the one proposed by COGR, AAU and APLU because while their recommendation would ameliorate concerns regarding the development of new courses, it does not address the implications created by the use of the terms "general scientific, mathematical, or engineering principles" and "commonly taught." Based on the preamble to the proposed rule, we do not believe BIS intends to alter the scope of the educational information exclusion currently available to institutions of higher

education under the EAR and for this reason we strongly urge BIS to retain the current language for which BIS and the university community have a shared understanding.

Definition of “Fundamental Research”

The definition of “fundamental research” is of critical importance to the University of Virginia and all institutions of higher education. The proposed rule adopts a definition of “applied research” taken from the Defense Federal Acquisition Regulations Supplement (DFARS) (48 CFR part 31.205-18) with an alternate definition adopting Office of Management and Budget (OMB) Circular A-11 language.

The University of Virginia finds the proposed excerpt from DFARS’ definition to be unacceptable, as it fails to clearly distinguish “applied research” from “development” activities. If the intent of the reform initiative and this proposed rule is to harmonize the EAR with the DFARS then we recommend BIS adopt the **full definition** of “applied research” found at 48 CFR part 31.205-18 which reads as follows:

*“Applied research means that effort which (1) normally follows basic research, but may not be severable from the related basic research, (2) attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, and (3) attempts to advance the state of the art. Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term *development*, defined in this subsection.” (48 CFR 31.205-18)*

The final statement, which was excluded from the proposed definition, crucially differentiates between “applied research” falling clearly within the scope of “fundamental research” and regulated “development” activities. The overwhelming majoring of applied research conducted by institutions of higher education is intended to advance the state of the art and be published rather than to develop a product, item or service, for sale.

If the ultimate goal is to clearly capture the intent of BIS in a simplified definition, the University of Virginia suggests following AUECO’s proposed revision, i.e., that ““fundamental research” means research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons”.

The University of Virginia currently uses §734.8(b) to make determinations regarding fundamental research by evaluating proposed research activities against paragraphs 2-6, and treats all activities that qualify as “fundamental research” provided all applicable conditions are met. To this end the University recommends BIS retain the specific language of §734.8(b).

“Fundamental research”, “technology”, and “software”

The proposed language in §734.8(a) states that “‘technology’ that arises during, or results from, fundamental research and is ‘intended to be published’” would not be subject to the EAR. This significant departure from the current language in §734.3(b)(3), under which “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR. The exclusion of “software” from the proposed rule would significantly complicate and restrict university research and represents a substantial change in applicability of the EAR. Under the proposed rule, natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, while a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions. We also note that the proposed rule refers to a note (which we were unable to locate) “to clarify that software and commodities are not ‘technology resulting from fundamental research’” but without this note we are unable to assess the full implications of the proposed change.

In some fields “software” is a direct product of academic research while in others “software” may be created by the researcher to conveniently accomplish a particular task. Regardless of the circumstance in which it is produced, when researchers intend to publicly disseminate such “software” and are under no sponsor imposed restrictions on dissemination, the EAR currently treats this source code as information that arose during, or resulted from, fundamental research and therefore excludes it from scope of the EAR. We contend that this interpretation is consistent with prior case law, specifically the finding of the Sixth Circuit Court of Appeals in *Junger v. Daley* where the court ruled that source code is protected by the First Amendment. Additional support for this position is provided by the ruling of the Ninth Circuit Court of Appeals in *Bernstein v. U.S. Department of Justice* where the court found that software source code was speech protected by the First Amendment and that the government's regulations (referring to the ITAR) preventing its publication were unconstitutional; the finding that dissemination of is protected expression should apply equally to the EAR.

The export definitions in §734.2(b) recognize the similarities between “software” and “technology”. We strongly urge BIS to incorporate the following modification, as recommended in the AUECO comment letter to this proposed rule, to §734.8:

§ 734.8 “Technology” and “software” that arises during, or results from, fundamental research.

(a) “Technology” or “software” that arises during, or results from, fundamental research and is ‘intended to be published’ is not “subject to the EAR.”

(b) Prepublication review. “Technology” or “software” that arises during, or results, from fundamental research is “intended to be published” to the extent that the researchers are free to publish the technology and software source code without restriction or delay. “Technology” that arises during, or results from, fundamental research subject to prepublication review is still “intended to be published” when:

Adoption of this language would continue the longstanding recognition by BIS that both “technology” and “software” arising during, or resulting from, fundamental research are outside the scope of the EAR.

Questions and Answers - Technology and Software Subject to the EAR

The University of Virginia urges BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. While we agree that the questions and answers are merely illustrative, their inclusion in the EAR lessens the likelihood that changes in interpretation will occur outside of the rulemaking process. These illustrative examples frequently inform export control decisions at universities and their removal result would increase uncertainty regarding the applicability of the EAR to fundamental research, publication, and educational instruction.

End to End Encryption Standard

The University of Virginia appreciates the additional clarity provided by listing activities that are not exports, reexports or transfers in §734.18. The exclusion of sending, taking or storing software and technology that is secured using end to end encryption from export activities is particularly welcome, as it will reduce the burden on faculty members and administrators traveling abroad. The flexibility provided by BIS via their proposal of a minimum standard of FIPS 140-2 or other similarly effective means is also appreciated as it provide us with the ability to use alternative means or to adopt new tools and/or techniques to enhance data protection as they become available rather than having to wait for a change in the regulations.

Effective Date of the Final Rule

Although the proposed changes do not modify the CCL, they will, if adopted as proposed, have a significant impact on regulatory burden for the University of Virginia and other institutions of higher education in the U.S. Industry sponsors, as well as many foundations supporting medical research, routinely require a limited time (typically less than 90 days) for prepublication review to ensure that sponsor-provided proprietary information is not inadvertently disclosed and to enable patent filing. U.S. universities have until now interpreted such requirements as being compatible with a fundamental research determination. If software that arises during, or results from, fundamental

research is not clearly excluded from the scope of the EAR (as is currently the case) existing research funding agreements will have to be reassessed to determine if controls will apply to software being written to enable the research or as a intended research output. These proposed changes as well as the proposed ITAR §120.49(b) Prepublication Review will require us to significantly modify our business practices associated with review, negotiation and management of sponsored research opportunities. The University of Virginia will not be able to meet the compliance obligations imposed by the addition of the prepublication review language of ITAR §120.49(b) and the reassessment of “software” arising during, or resulting from, fundamental research within 30 days of the publication date of a final rule necessitating these changes in practice; therefore, we request that BIS provide at minimum a 6 month delay in effective date, and limit applicability of the new provisions to new research funding agreements entered into on or after the effective date of the Final Rule.

The University appreciates the opportunity to provide comments on these proposed changes.

Sincerely,

A handwritten signature in blue ink, reading "Kelly Hochstetler". The signature is fluid and cursive, with the first name "Kelly" written in a larger, more prominent script than the last name "Hochstetler".

Kelly Hochstetler, Ph.D.
Director, Finance Outreach and Compliance



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0033
Tracking Number: 1jz-8kcm-9znn

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Matt Watson

Comment

1st Amendment, you have no authority to restrict it.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0034

Tracking Number: 1jz-8kcm-nlt8

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

Show More Details 

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

This is a blatant violation of freedom of speech.

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am pleased to provide comments to the proposed changes to the definitions in the Export Control Administration Regulations (EAR).

Texas A&M University is located in College Station, Texas with branch campuses in Galveston, Texas and Doha, Qatar. It is the flagship institution of The Texas A&M University System and home to more than 50,000 students. It is among the nation's five largest universities, and is one of a select few academic institutions in the nation to hold triple federal designations as a land-grant, sea-grant and space-grant university. Texas A&M University is also member of the prestigious Association of American Universities and ranks in the top tier of universities nationwide in research expenditures with more than \$820 million – attracting prominent, respected scholars and researchers from around the world.

We are pleased to have the opportunity to comment on the proposed Revisions to the Definitions in the Export Administration Regulations (EAR) and the corresponding changes to the International Traffic in Arms Regulations (ITAR). While we appreciate the efforts that have been made to harmonize export control related definitions, we believe that the proposed changes, if adopted, will have a significant impact on Texas A&M University. Highlighted below are our specific concerns.

Fundamental Research and Applied Research

The proposed definition of “fundamental research” using the language of NSDD-189 in the EAR and the ITAR is consistent with U.S. academic institutions’ understanding of the concept. The proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18) with an alternate definition adopting OMB Circular A-11 language.

The OMB Circular A-11 language reads: “applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met”. This language is well understood by universities in the context of

reporting on federal expenditures to NSF, and we favor the adoption of this commonly used definition.

If the DFARS definition is adopted, we suggest that the definition of “applied research” be further clarified by including the rest of 48 CFR part 31.205-18 – “Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development, defined in this subsection.” — the “for sale” criterion will help to clearly distinguish between “applied research” and “development” activities.

With regard to BIS’ proposed alternate definition: “fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. We assume that this simpler definition would not alter other wording in the proposed rule permitting prepublication review under specific circumstances within the fundamental research domain. While we generally favor the simplified definition, it would be helpful if a note were added to illustrate what is and is not non-proprietary, or alternately for the term to be defined. This will clarify any ambiguity about what is and what is not “non-proprietary”.

We strongly recommend that the specific criteria for university based research currently found in §734.8(b) be retained in the EAR. The criteria is used by universities to make determinations as to the applicability of fundamental research by evaluating proposed research activities using paragraphs 2 -6. The removal of the specific criteria will create interpretive uncertainty. That said, Texas A&M University appreciates that the proposed definition of “fundamental research” clarifies the broad applicability of the concept regardless of organization type or location.

Technology, Software and Fundamental Research

Under the proposed §734.8(a), “technology” that arises during, or results from, fundamental research and is “intended to be published” would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which “publicly available technology and software... [that] arise during, or result from, fundamental research” are not subject to the EAR.

The proposed rule refers to a proposed note “to clarify that software and commodities are not “technology resulting from fundamental research” (although we were unable to locate the note). This change would significantly complicate and restrict university research; while natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions. “Software” resulting from university research is “published” as well as “technology”, as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology. We strongly recommend that the proposed §734.8(a) be revised as follows:

§ 734.8 “Technology” and “software” that arises during, or results from, fundamental research.

- (a) “Technology” or “software” that arises during, or results from, fundamental research and is ‘intended to be published’ is not “subject to the EAR.”
- (b) Prepublication review. “Technology” or “software” that arises during, or results, from fundamental research is “intended to be published” to the extent that the researchers are free to publish the technology and software source code without restriction or delay. “Technology” that arises during or results from fundamental research subject to prepublication review is still “intended to be published” when:

Proposed Changes to Educational Information

We believe that the proposed change to the current definition of educational information will significantly impact universities by potentially narrowing the scope of the applicability of the exclusion.

The current §734.9 defines “educational information” as information released by instruction in catalog courses and associated teaching laboratories of academic institutions, and §734.3(b)(3)(iii) excludes such information from the scope of the EAR. In the proposed rule, the definition of “educational information” is removed, and §734.3(b)(3)(iii) excludes information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution.

We believe that the proposed change adds uncertainty and restricts university research. Like other universities, Texas A&M University offers many catalog courses that include hands on design laboratories, particularly as capstone experiences. It is unclear whether or not the content of these courses, which would have previously been treated as “educational information” would become subject to the EAR by virtue of including more than general principles.

Universities do not discriminate on the basis of citizenship or national origin in academic programs. Education at universities is by nature open, with the opportunity to participate limited only by required prerequisites. A narrow interpretation of the revised §734.3(b)(3)(iii) would inhibit the ability of U.S. universities to develop new courses in emerging areas of science and engineering critical to employability of their graduates and the future competitiveness of the industrial sector. Therefore, we suggest that the qualifier “concern general scientific, mathematical, or engineering principles commonly taught in schools” be removed and that the simpler “is released by instruction in catalog courses and associated teaching laboratories of academic institutions” be retained for §734.3(b)(3)(iii). As an alternative, we believe changing the proposed description to “information and “software” that concern general scientific,

mathematical, or engineering principles commonly taught in schools and /or released by instruction in a catalog course or associated teaching laboratory of an academic institution” would describe educational information more fully without narrowing the scope of the exclusion.

Questions and Answers in Supplement No. 1 to part 734

We urge BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. While we agree that the questions and answers are illustrative, inclusion of them in the EAR removes the uncertainty created by changes due to interpretive differences without benefit of the rulemaking process. We are concerned that removal of the questions and answers, which we use to guide export control decisions, would create increased uncertainty in our application of key concepts including fundamental research, publication, and educational instruction. It should be noted that other parts of EAR contain important regulatory information (e.g., Supplement No. 1 to part 740).

End-to-end encryption in the proposed revision of the definition of “Activities that are Not Exports, Reexports, or Transfers,”

We believe the addition of §734.18 listing activities that are not exports, reexports or transfers is a useful addition to the EAR. In particular, the exclusion of sending, taking or storing software that is secured using end to end encryption from export activities is welcome to the academic research community as it will reduce the faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad.

Proposed Effective Date

While the revised definitions do not make changes to the USML or the CCL, as written they have a significant impact on regulatory burden for U.S. universities. Most industry sponsors of university research, as well as many foundations, require limited time prepublication review to prevent the inadvertent disclosure of sponsor proprietary information and to permit seeking of patent protection as applicable. U.S. universities have until now interpreted such reviews as within the scope of fundamental research. If the proposed changes to ITAR §120.49(b) Prepublication Review go to final rule without changes, Texas A&M University, like many other universities, will need to significantly change their business practices associated with review and negotiation of sponsored research agreements as well as the management of access to sponsored research. These changes will require implementation of new procedures to determine applicability of the ITAR to fundamental research with prepublication review, implementation of technology control plans and submission of license applications for the participation of foreign nationals in the research, monitoring of those plans, and eventual removal of the plans once the prepublication review has occurred, as well as revised export compliance training for affected departments on campus. Importantly, such review would be required retrospectively for current projects. These procedures will also require additional staffing for export compliance. Texas

Ms. Hillary Hess
August 3, 2015
Page 5 of 5

A&M University favors as much lead time as possible for implementation and suggests, at a minimum, a 6 month delay in the effective date, and further that the revised regulations be applicable only to new sponsored research begun after the effective date of the Final Rule.

Thank you for the opportunity to provide comments on the proposed changes.

Sincerely,



Dr. Glen A. Laine
Vice President for Research



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0036
Tracking Number: 1jz-8kcn-tg51

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

This is a clear abridgment of the First Amendment. It is beyond ill-advised, it is inflammatory and dangerous. Remember your oath.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment

This is a clear abridgment of the First and Second Amendment. It is beyond ill-advised, it is inflammatory and dangerous.

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0037

Tracking Number: 1jz-8kcn-z23s

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Charles Roberts



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0038

Tracking Number: 1jz-8kcn-wi68

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

Another ridiculous attempt at anything related to firearms. Trying to take away rights to speak about firearms, on forums, is just sad. A back door attack on our 1st and 2nd amendment rights, knowing that it will only open doors to other "regulations". I oppose this and will continue to oppose any regulations that are an attempt to strip myself and fellow Americans of our rights.

Ad Hoc Coalition for Effective Export Control Reform
1717 Pennsylvania Avenue, N.W. – Suite 1025
Washington, DC 20006

August 3, 2015

VIA E-MAIL (publiccomments@bis.doc.gov AND DDTCTPublicComments@state.gov)

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

Mr. C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
Washington, DC 20522

REF: RIN 0694-AG32 (BIS) AND RIN 1400-AD70 (DDTC)

RE: Comments on Proposed Revisions to Certain EAR and ITAR Definitions

Dear Ms. Hess and Mr. Peartree:

The Ad Hoc Coalition for Effective Export Control Reform (“CEECCR”)¹ appreciates the opportunity to comment on the proposed rules published by the U.S. Department of Commerce, Bureau of Industry and Security (“BIS”) and the U.S. Department of State, Directorate of Defense Controls (“DDTC”) on June 3, 2015 (80 Fed. Reg. 31505 and 80 Fed. Reg. 31525, respectively) concerning proposed revisions to certain definitions in the Export Administration Regulations (“EAR”) and the International Traffic in Arms Regulations (“ITAR”) (individually, the “BIS Proposed Rule” and the “DDTC Proposed Rule,” and collectively, the “June 3 Proposed Rules”).

The CEECCR believes that the expressed aims, scope, and substance of the June 3 Proposed Rules are linked to those set forth in the proposed rule on Wassenaar Arrangement 2013 Plenary Agreements Implementation that BIS published on May 20, 2015 (80 Fed. Reg. 28853) (RIN 0694-AG49) (the “May 20 Proposed Rule” or the “Wassenaar Arrangement Implementation Rule”). Accordingly, Section XI contains comments relating to the May 20 Proposed Rule for consideration by BIS.

¹ The Ad Hoc Coalition for Effective Export Control Reform (“CEECCR”) includes the following individuals: Geoffrey M. Goodale, Managing Member, Trade Law Advisors, PLLC (Washington, DC); Andrea Fekkes Dynes, Staff Vice President and Associate General Counsel, General Dynamics (Falls Church, VA); Kay C. Georgi, Partner, Arent Fox LLP (Washington, DC); Gwendolyn W. Jaramillo, Partner, Foley Hoag LLP (Boston, MA); Jonathan M. Meyer, Attorney-at-Law (New York, NY); Jason I. Poblete, Partner, Poblete Tamargo LLP (Washington, DC); Christopher B. Stagg, Partner, Stagg Noonan LLP (Washington, DC); Roland L. Trope, Partner, Trope & Schramm LLP (New York, NY); Michael L. Burton and Douglas N. Jacobson, Members, Jacobson Burton PLLC (Washington, DC) (on behalf of TRW Automotive U.S. LLC d/b/a ZF TRW and other firm clients). The comments set forth in this submission are fully supported by these individuals, but they do not necessarily reflect the views of the entities by which they are employed or whom they represent.

The CEECR applauds the U.S. Government's efforts to amend the EAR and the ITAR as part of the Obama Administration's ongoing Export Control Reform ("ECR") initiative. It is quite apparent from the text of the June 3 Proposed Rules, from comments that agency officials have made regarding on the June 3 Proposed Rules, and from the experience of our members in analyzing the June 3 Proposed Rules that much thought went into the proposed definitions that are referenced in the June 3 Proposed Rules.

In our view, many of the proposed definitions that are set forth in the June 3 Proposed Rules represent significant improvements over earlier versions of proposed definitions that have previously been issued by BIS and DDTC. However, it is the CEECR's view that the proposed definitions for certain terms under the EAR and ITAR could be further improved by making the changes or clarifications that are recommended below.

I. "Export" and "Reexport" Under the EAR and the ITAR

A. "Subject to the EAR" in Proposed EAR § 734.13 and EAR § 734.14

In the BIS Proposed Rule, the term "subject to the EAR" is not referenced in the proposed definition of "export" under EAR § 734.13, whereas that term has been used in connection with the current definition of "export" under the existing EAR. For purposes of clarity, the CEECR recommends that the term "subject to the EAR" be added in the applicable places in the proposed definition for "export" under EAR § 734.13. Specifically, we propose that the term "of items subject to the EAR" be inserted after the words "shipment or transmission" in subsection (a)(1). We also propose adding the words "subject to the EAR" before the words "to a foreign national" in subsection (a)(2), before the words "in clear text" and the words "to a foreign national" in subsection (a)(6), and before the words "to a foreign national" in subsection (b).²

Similarly, we recommend adding the term "subject to the EAR" and additional changes to proposed EAR § 734.13(c) so that the text would read as follows.

The export of an item subject to the EAR that will transit through a country or countries to a destination country, or will be transshipped in a country or countries to a destination country, or are intended for export to the ~~new~~ destination country, is deemed to be an export to the ~~new~~ destination country and not to the countries of transit or transshipment.

This recommended text also has the benefit of adding clarity by substituting the term "destination country" for the term "new country" that exists in the proposed definition referenced in the BIS Proposed Rule and by adding the phrase or replacing the term "new country" in several places in sections 13(c) and 14(c) with the "and not to the countries or transit or transshipment" at the end of the proposed definition.

² See also Section I.B.1 for additional recommended changes to proposed EAR § 734.13(a)(6) and related proposed EAR § 734.14(a)(4).

For the reasons discussed above, the CEECR also recommends that conforming changes along the lines discussed above be made to the applicable parts of the proposed definition of "reexport" in proposed EAR § 734.14. Specifically, the CEECR proposes that the term "subject to the EAR" be added after the words "shipment or transmission" in subsection (a)(1), before the words "to a foreign national" in subsection (a)(2), and before the words "to a foreign national" in subsection (a)(4). We note that subsections 734.14(b) and (c) already include the phrase "subject to the EAR", as we have proposed should be the case in the corresponding subsections of proposed section 734.13.

B. Proposed New Definition for Export – Release or Transfer of Decryption Keys, Network Access Codes, Passwords, etc.

1. Proposed EAR § 734.13(a)(6)
(And Conforming Changes to Proposed EAR § 734.14(a)(4))

Under the BIS Proposed Rule, the proposed definition for "export" under EAR § 734.13(a)(6) reads as follows:

(6) "releasing or otherwise transferring decryption keys, network access codes, passwords, 'software,' or other information with 'knowledge' that such provision will cause or permit the transfer of other 'technology' in clear text or 'software' to a foreign national." (emphasis added).

The CEECR understands that the BIS does not intend to include in the definition of export the mere act of releasing decryption keys, network access codes, passwords, 'software,' or other information but rather intends to focus on those situations where an individual undertakes such an act with knowledge that it will cause and result in a transfer of the EAR-controlled technology or software. However the word "permit" is overly broad as any release of decryption keys, network access codes, passwords, 'software,' or other information could technically "permit" such access.

The CEECR also believes that the terms "cause or permit" may be overly broad with regard to access issues and do not match the "result in" terminology in proposed EAR § 764.2(1). We believe the terms "cause or permit" could be interpreted more broadly than BIS intends, to include scenarios in which, for example: (a) a person has a decryption key stored in a briefcase in the same room as a foreign national who does not even know that the decryption key is in the briefcase because this might in theory "permit" the foreign national to have access to the decryption key; or (b) during a factory tour a foreign person receives access to an area adjacent to an area containing controlled information and breaks into the area containing controlled information. Under the latter scenario, taking the person on the factory tour may be one of the "causes" of the break-in, but it is certainly not a "sufficient cause." As such, the CEECR favors using the term "**result in**" instead of "cause or permit."

In addition, the CEECR believes that using the qualifier "in clear text or 'software'" within proposed paragraph (a)(6) could result in some confusion. This is because some exporters might not think drawings, diagrams, specifications or other non-prose information is included within the term "clear text" or "software." In the preamble to the BIS Proposed Rule, BIS has

indicated that “[t]he meaning of ‘clear text’ in the proposed definition is no different than an industry standard definition, e.g., information or software that is readable without any additional processing and is not encrypted. Comments are encouraged regarding whether a specific EAR definition of the term is warranted and, if so, what the definition should be.” While the term “clear text” may have an industry definition within the computer/information security industry, we are uncertain that it has a uniform meaning in that industry, or that its meaning is generally known within other industries.

For the reasons discussed above, the CEECR recommends that proposed EAR § 734.13(a)(6) be revised to read, in relevant part, as follows:

(6) “releasing or otherwise transferring decryption keys, network access codes, passwords, ‘software,’ or other information with ‘knowledge’ that such provision will result in cause or permit the transfer of other ‘technology’ in unencrypted format ~~clear text~~ or ‘software’ in source code format to a foreign national.”³

Alternatively, if BIS wishes to retain the term “clear text” in proposed EAR § 734.13(a)(6), the CEECR proposes that BIS define the term “clear text” to mean “information that is readable without further decryption.” In addition, the CEECR recommends that BIS provide additional clarification regarding the term “software” since BIS is proposing to exclude from the definition of “export” transfers of object code to foreign nationals. See proposed EAR § 734.13(a)(2).

Furthermore, for all of the reasons discussed above, the CEECR recommends that conforming changes along the lines of those proposed above be made to the proposed definition of “reexport” in proposed EAR § 734.14(a)(4).

2. Proposed ITAR § 120.17(a)(6)
(And Conforming Changes to Proposed ITAR § 120.19)

Like the expansion of the definition of “Export” under the EAR, the new proposed ITAR § 120.17(a)(6) addresses the release or transfer of decryption keys, network access codes, passwords, software to a foreign person. However, the proposed ITAR definition differs significantly from the proposed EAR in the following two respects. First, unlike the EAR, the ITAR definition includes in the definition of “Export” the mere act of “providing physical access that would allow access to other technical data.” Second, unlike the EAR, the ITAR definition includes in the definition of “Export” situations where **no** technical data has been or will be transferred to a foreign person. In the preambles to the referenced proposed rules, both DDTC and BIS have requested input from the public regarding the different formulations for this control.

³ See also Section I.A. for additional recommended changes to proposed EAR § 734.13(a)(6) and related EAR § 734.14(a)(4).

The CEECR believes that the proposed revised definition for “Export” in ITAR § 120.17(a)(6) is overly broad because, as written, it captures scenarios where a foreign person has been provided mere physical access to decryption keys, network access, or passwords but no actual transfer of ITAR-controlled technical data occurs. See similar discussion above relating to EAR § 734.13(a)(6) for examples of situations where mere physical access does not result in any export of controlled information, as a matter of fact. As written, the definition would capture all situations where “access” was provided (perhaps by mistake), regardless of other facts such as period of time involved (unfettered long-term access versus short-term access) and the reality of whether technical data was actually transferred to a foreign person as a matter of fact.

For all the reasons discussed above, the CEECR recommends that proposed ITAR § 120.17(a)(6) be revised to read as follows:

(6) Releasing or otherwise transferring ~~information such as~~ decryption keys, network access codes, passwords, software, or other information with knowledge that such provision will result in the transfer of other in unencrypted format or ‘software’ in source code format to a foreign person.

Furthermore, for all of the reasons discussed above, the CEECR recommends that conforming changes along the lines of those proposed above be made to the proposed definition of “reexport” in ITAR § 120.19.

II. “Release” Under the EAR and the ITAR

A. Proposed EAR § 734.15

The CEECR commends BIS for seeking to create a new definition for the term “release” under proposed EAR § 734.15. As noted in the preamble to the BIS Proposed Rule, the proposed new definition of “release” would only apply to inspections of an item or applications of knowledge or technical experience that “actually reveal controlled technology or source code” to a foreign national. See 80 Fed. Reg. 31505, 31508 (June 3, 2015). The preamble goes on to explain that “merely seeing equipment does not necessarily mean that the seer is able to glean any technology from it and, in any event, not all visible information pertaining to equipment is necessarily ‘technology’ subject to the EAR.” We believe the language in the definition of release is reasonably clear when read together with the preamble to the proposed rule.

However, after the new definition becomes effective, it may not be completely clear when reading the definition alone what BIS intended by the term “inspection”, and by the two references to conduct that “reveals” technology or source code subject to the EAR to a foreign national. To ensure the language in the EAR is clear on its face, without also having to find and review the preamble to the proposed rule, we recommend that BIS take the following actions:

- (a) replace the phrase “visual or inspection” with “visual or other examination” or “close inspection by visual or other means”; and
- (b) to replace the two instances of the term “reveals” with the term “actually reveals” or “actually conveys”.

In addition, for the reasons discussed above under section I.A, the CEECR proposes adding the words “subject to the EAR” after the words “by a foreign national of items” in proposed EAR § 734.15(a)(1) and before the words “in the United States or abroad” in proposed EAR § 734.15(a)(2).

B. Proposed ITAR § 120.50

The CEECR agrees with the decision by DDTC to create and define the term “release” under proposed ITAR § 120.50 and for taking actions to make that definition consistent with the definition of “release” under proposed EAR § 734.15. For the reasons discussed above, the CEECR also recommends that conforming changes along the lines discussed above relating to EAR § 734.15 be made to the applicable parts of proposed ITAR § 120.50, except that the term “subject to the EAR” language should not be added anywhere in proposed ITAR § 120.50.

III. “Activities that are not exports reexports, or transfers” Under the EAR and ITAR

A. Proposed EAR § 734.18

Under proposed EAR § 734.18(a)(4), certain activities are excluded from the proposed definitions of export, reexport and transfer, including:

(4) sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, . . . , or other similarly effective means; and

(iv) Not stored in a country listed in Country Group D:5 (*see* Supplement 1 to part 740 of the EAR) or in the Russian Federation. (emphasis added).

The CEECR recommends that BIS clarify its intention that an electronic transmission (*e.g.*, an e-mail) which may *transit* a country in Country Group D:5 or in the Russian Federation, and which otherwise meets the requirements of subsection (4), falls within the scope of activities that are not exports, reexports, or transfers. Specifically, such electronic transmissions are not “stored” in a country listed in Country Group D:5 or the Russian Federation. Thus, for example, a party sending an email that contains technology subject to the EAR, using end-to-end encryption and meeting the other requirements of subsection 4 can rely on such an electronic transmission *not* to constitute an export, reexport or transfer provided the party does not know that the email server is located in Country Group D:5 or in the Russian Federation.

B. Proposed ITAR § 120.52

Under proposed ITAR § 120.52, certain activities are excluded from the proposed definitions of export, reexport and transfer, including:

(4) sending, taking, or storing technical data or software that is:

(i)Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications; and

(iv) Not stored in a country proscribed in §126.1 of this subchapter or the Russian Federation. (emphasis added)

The CEECR recommends that DDTC clarify its intention that an electronic transmission (such as an email) which may *transit* a country proscribed in §126.1 of this subchapter or the Russian Federation, and which otherwise meets the requirements of subsection (4), falls within the scope of activities that are not exports, reexports, or retransfers. Specifically, such electronic transmissions are not “stored” in a country proscribed in §126.1 of this subchapter or the Russian Federation. Thus, for example, a party sending an email that contains unclassified technical data, using end-to-end encryption and meeting the other requirements of subsection 4 can rely on such an electronic transmission *not* to constitute an export, reexport or transfer provided the party does not know that the email server is located in a country proscribed in ITAR § 126.1 or in the Russian Federation.

IV. “Activities that are not ‘deemed reexports’” Under the EAR

A. The Term “Is Certain” in Proposed EAR § 734.20

In the BIS Proposed Rule, proposed EAR § 734.20(a)(2) states that a “deemed reexport” does not occur if an entity:

[i]s certain that the foreign national’s most recent country of citizenship or permanent residency is that of a country to which export from the United States of the “technology” or “source code” at issue would be authorized by the EAR either under a license exception, or in situations where no license under the EAR would be required.” (emphasis added)

Significantly, the term “certain” is not defined in the current EAR or in the BIS Proposed Rule, and as such, use of the term may cause confusion. Moreover, as a practical matter, it is not generally possible for companies to achieve 100% certainty about the citizenship or residency status of nationals of their own country, let alone dual or third country nationals.

The CEECR does not believe that the intent of BIS was to set an impossibly high standard or to create a strict liability standard under which a company may be found liable for improperly reexporting to a dual/third country national even if the company reasonably relies on ordinary identification documents, passports, visas, etc. to determine the nationality or residency of an individual. However, if that was BIS’s intent, we do not believe that such a strict liability standard is appropriate. Non-U.S. entities that receive controlled items and technology should be allowed to use ordinary means of determining the citizenship or residency of an individual. Requiring them to achieve “certainty” could effectively stifle cooperation with close allies because it would make it far harder for companies inside close U.S. allies U.S. to collaborate with U.S. companies on export-controlled projects, which collaboration it is a major objective of export reform to promote.

For the reasons discussed above, the CEECR recommends that the term “has knowledge” be substituted for the term “is certain” in applicable places in proposed EAR § 734.20(a)(2). The CEECR believes that the term “has knowledge” is more clear (and consistent with other portions of the EAR) than the term “is certain” and is more in line with the objectives of BIS.

B. Proposed EAR §§ 734.20(b)-(c)

Proposed subsections (b) and (c) of proposed EAR § 734.20 exclude from the concept of “deemed reexport” other releases of technology or source code, by an entity outside the United States, to foreign national employees, if the employee is a national only of a country in Country Group A:5, or if certain specified clearances, screening measures or safeguards are in place. One of the requirements for the subsection (b) and (c) exclusions from the concept of “deemed reexport” is that the “release of ‘technology’ or ‘source code’ takes place entirely within the physical territory” of a country in Country Group A:5, or the country in which the entity releasing the technology or source code “is located, conducts official business, or operates.”

Modern electronic communications often involve conduct falling within the definition of “release” that occurs in more than one location. It will often be the case that a release of U.S.-origin technology or software could be said to take place partially within the United States and partially within the country in which the foreign person employee is located. In each case we believe that it would be consistent with the purposes of these exceptions, and would make them more practical and straightforward to apply, if the restriction on the location of the release also included the physical territory of the United States. For these reasons, the CEECR proposes that the words “or within the physical territory of the United States” be added at the end of each of subsections (b)(4) and (c)(3) of proposed EAR § 734.20.

V. **“Knowledge” and “Violations” Under the June 3 Proposed Rules**

A. **Proposed EAR § 764.2(l)**

Under proposed EAR § 764.2(l), it is stated that the “release” or transfer of data security-related information (*e.g.*, decryption keys, network access codes, or passwords) “with ‘knowledge’ that the release will result, directly or indirectly, in an unauthorized export, reexport, or transfer of the ‘technology’” will constitute a violation to the same extent as a violation in connection with the export of the controlled “technology” or “software.” The CEECR supports the inclusion of a knowledge qualifier in this proposed new CEECR of the EAR.

However, the CEECR notes that the terms “directly or indirectly” may be confusing when speaking of decryption keys and access issues. This is because transferring or releasing an encryption key or granting access is inherently only an indirect way to export technology or software. Use of the term “indirect” here raises numerous questions, such as (a) whether failing to secure all possible vulnerabilities against hackers (an impossibility) would in and of itself constitute a violation (because there is knowledge that this could “indirectly” result something), and (b) whether failing to properly train an employee who falls victim to a “phishing” attack is a violation (because there is knowledge that a foreign national might “indirectly” use the attack to steal export controlled technology or software). Accordingly, the CEECR proposes that the terms “directly or indirectly” be deleted from proposed EAR § 764.2(l).

B. **Inconsistency of Statements on “Knowledge” in the Preamble and the BIS Proposed Rule**

The BIS Proposed Rule indicates that the term “knowledge” within the definition of “export” would limit the scope of the term “export.” However, in the preamble to the BIS Proposed Rule, BIS raises the issue of whether a party that acts without “knowledge” may still be guilty of violations. BIS states that the proposed rule would:

Add text prohibiting the release or other transfer of information (*e.g.*, decryption keys, passwords or access codes) with knowledge that such release or other transfer will result in an unauthorized export, reexport or transfer of other technology or software. This addition provides specific grounds for bringing charges with respect to one particular type of misconduct. However, existing EAR provisions, including the prohibition on causing, aiding or abetting a violation of the EAR or license, authorization or order could be used to bring charges for that same type of misconduct.

80 Fed. Reg. at 31513 (emphasis added).

The CEECR is concerned that the underlined language above is in tension with the stated intent to use a knowledge qualifier within the proposed definitions of “export” and “reexport” set forth in the BIS Proposed Rule. The above language appears to say that the “same type of conduct” that is not a violation because there is no “knowledge” of a transfer could nevertheless be considered “causing, aiding or abetting a violation.” Our understanding is that BIS’s intention

was to say that “causing, aiding or abetting a violation of the EAR or license, authorization or order could be used to bring charges for other or related conduct even if there is no “knowledge” that a transfer will occur with respect to transfer of a particular technology or software.” Accordingly, the CEECR requests that BIS provide clarification on this issue in the final rule.

C. Proposed ITAR §§ 127.1 (a)(6) and §127.1 (b)(4)

The DDTC Proposed Rule would add two new subsections describing activities that constitute violations of the ITAR.

- Proposed ITAR § 127.1(a)(6) would make it unlawful “to export, reexport, retransfer, or otherwise make available to the public technical data or software if such person has knowledge that the technical data or software was made publicly available without an authorization described in CEECR 120.11(b) of this subchapter. (emphasis added).
- In contrast, proposed ITAR § 127.1(b)(4) would make it unlawful “to release or transfer information, such as decryption keys, network access codes, or passwords that would allow access to other technical data in clear text or to software that will result, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software. Violation of this provision will constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software.” (emphasis added)

In proposed ITAR § 127.1(a)(6), DDTC does not penalize the act where an individual exports/reexports/retransfers information obtained from a public resource, such as the Internet, when such individual does not have knowledge that information is subject to ITAR. Rather, DDTC criminalizes the act where the individual exports, reexports, transfers such information with knowledge that it contains ITAR-controlled technical data or software which was made publicly available without an authorization.

However, proposed ITAR § 127.1(b)(4) does not similarly address those situations where an individual acts with or without knowledge; but rather it equally penalizes both acts. As a result, for example, an individual who provides (perhaps mistakenly) a network password to a foreign person without knowledge that it will result in access to technical data, would be liable for such acts – *even when no actual export of ITAR-controlled technical data results.*

The strict liability approach taken in proposed ITAR § 127.1(b)(4) is inconsistent with proposed ITAR § 127.1(a)(6) (which would result in no liability for mistaken acts, even though an actual export of ITAR-controlled technical data would result). Proposed ITAR § 127.1(b)(4) also would be inconsistent with proposed EAR § 764.2(1), which has a knowledge requirement similar to that of ITAR § 127.1(a)(6). *See* discussion above in Section V.A.

The CEECR urges DDTC to revise proposed ITAR § 127.1(b)(4) to be consistent with proposed ITAR § 127.1(a)(6) in terms of including a knowledge or scienter requirement, which also would be consistent with proposed EAR § 764.2(1). Specifically, we recommend that proposed ITAR § 127.1(b)(4) be revised as follows to make it unlawful:

“to release or transfer information, such as decryption keys, network access codes, or passwords **with knowledge that such provision will result**, directly or indirectly, in an unauthorized export, reexport, or retransfer of the technical data in clear text or software.”

In addition, we propose that a safe harbor be created for instances in which the release or transfer of decryption keys, network access codes, or passwords does not actually result in the disclosure of technical data in clear text or software to a foreign person. We recommend that the following language be added to create such a safe harbor:

“Violation of this provision will be **presumed to** constitute a violation to the same extent as a violation in connection with the export of the controlled technical data or software **unless the exporter can establish to the Department’s satisfaction that the release or transfer of the decryption keys, network access codes or passwords, did not result in the actual access to technical data in clear text or to software by a foreign person.**”

VI. **“Required” and “Peculiarly Responsible” Under the BIS Proposed Rule**

A. **Proposed Definitions of “Required” and “Peculiarly Responsible” Under EAR § 772.1**

The BIS rule adds a definition to “required” stating that the term refers “only to that portion of ‘technology’ and ‘software’ that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.” The BIS then defines “peculiarly responsible” by using a catch and release technique employed under the “specially designed” section of the EAR and ITAR.

The CEECR believes that, due to the unique nature of technology and software, using the “catch and release” technique is a both significant departure from the EAR’s General Technology Note and an expansion of the controlled technology and software that will no longer be based on the technology or software being responsible for achieving control parameters.

The current EAR contain an element of causality in its definition of “required” in the following example, which is maintained in the current proposed definition of required:

For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example,

technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

In other words, even though technologies A, B and C are used to produce controlled product X, because they contribute nothing to making product X operate at or above 400 MHz – the control level – they are not controlled. In other words, to use plain English,

- A, B and C are not “required” – they are not “wanted, needed or called for” to use the Webster’s definition⁴ -- to produce that characteristic;
- A, B and C are also not “peculiarly responsible” – they are not “exclusively”⁵ “answerable as the primary cause motive or agent”⁶

But if we use the new ‘catch and release’ definition proposed for “peculiarly responsible,” all three technologies are “caught” because they are “used in or for use in the development, production or use” of the controlled item in question. And there is no guarantee that they will be “released” under (b)(3)-(b)(6). The technologies/software may only be used in or for use in the development or production the controlled item and not an EAR99 or AT-controlled item that is in “production” – not because they cause the properties that are the reason for the control – but simply because they are not used elsewhere. And as a lesser technology or software, there may not be the design history or documentation necessary to meet the other reasons for release. In short, the catch and release may result in over-control of the A, B and C types of technology and software that are not important to the reasons for control, but just happen to be for use in or for use in the development production or use of the controlled item.

The CEECR believe that the technologies that the BIS seeks to control are those that can usefully be thought of as a “but-for” cause of an item achieving a specified level or threshold of performance. In the above-example, technologies “D” and “E” would qualify as “but-for” causes of a product “X” operating at or above 400 MHz. The focus on the “but-for” causes of performance is lost in the “catch and release” definition proposed for “peculiarly responsible.” Whereas the use of a “but-for” cause approach would be far easier for exporters to understand and implement, would result in a more intuitive and consistent definition of “peculiarly response”, and would avoid extending the control to technologies for which there would not appear to be a need or reason for control.

It should also be noted, that, by eliminating the causal link between the

⁴ Webster’s New International Dictionary of the English Language, 2117 (1942) (to “require” is “to demand or exact as necessary or appropriate; hence, to want; to need; to call for...” (hereinafter “Webster’s”).

⁵ Webster’s at 1801 (defining “peculiar” as an “exclusive property or privileged . . .”)

⁶ Webster’s at 2124 (defining “responsible” as “answerable as the primary, cause, motive, or agent, whether good or evil, creditable or chargeable with the result.”)

technology/software and the controlled commodity, the catch and release definition is changing the definition from that found in the dictionary – and the Wassenaar Arrangement (which does not define the term “peculiarly responsible”) to a very different definition found in neither the dictionary nor the Wassenaar Arrangement.

Put another way, just because a technology or software is used in or for a controlled item, and is not used in or for a non-controlled item (according to the proposed “catch and release” definition), does not mean that the technology or software is “wanted, needed or called for,” to use the Webster’s definition of “required,” or “exclusively” “answerable as the primary cause motive or agent,” to use the Webster’s definition of “peculiarly responsible” for making the item controlled. In short, the proposed definition might well cause the United States to interpret the term significantly differently than the other Wassenaar Members.

Finally, the CEECR respectfully submits that the catch and release principals of “specially designed” are much more easily applied to parts, components, attachments and accessories, than it is to technologies. Due to its nature, it is more difficult to determine which technologies are used in different products, making the release part of the task particularly difficult to apply in real life.

In light of these concerns, the CEECR recommends that BIS omit the “catch and release” definition of “peculiarly responsible” and allow exporters to continue to rely on the dictionary definitions of “peculiarly responsible” and the A,B,C,D and E example provided in the “required” definition.

VII. “Required” Under the DDTC Proposed Rule

A. ITAR § 120.46

The DDTC Proposed Rule adds proposed ITAR § 120.46, stating that the term “required” refers “only to that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.” There are several recommendations that the CEECR wishes to make to this proposed definition of “required.”

As an initial matter, the CEECR notes that proposed ITAR § 120.46 does not make reference to “software.” Given that the definition of “required” under proposed EAR § 772.1 makes reference to both “technology” and “software,” we believe that the omission of the term “software” in proposed ITAR § 120.46 was an inadvertent error on the part of DDTC. Accordingly, the CEECR recommends that DDTC include the term “software” in the proposed definition of “required” when final rule is issued.

Second, for the same reason set forth above, the CEECR believes that DDTC should BIS omit the “catch and release” definition of “peculiarly responsible” and allow exporters to continue to rely on the dictionary definitions of “peculiarly responsible.”

If DDTC continues to use the “catch and release” definition of “peculiarly responsible,” however, the CEECR has the following suggestions.

First, the CEECR believes that proposed Paragraph 5 to proposed Note 3 to paragraph (a) of proposed ITAR § 120.46 should be revised. Proposed Note 3 to paragraph (a) to proposed ITAR § 120.46 states that technical data is peculiarly responsible for achieving or exceeding controlled performance levels, characteristics or functions “if it is used in or for use in the development . . . , production . . . , operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article unless . . . 5. It was or is being developed for use in or with general purpose commodities or software (*i.e.* with no knowledge that it would be for use in or with a particular commodity)” (emphasis added).

For consistency and clarity, the CEECR recommends that DDTC revise Paragraph 5 to proposed Note 3 to paragraph (a) of proposed ITAR § 120.46 by substituting the phrase “defense article” for the phrase “particular commodity.” There are several reasons why such action would be beneficial.

First, we note that DDTC’s primary interest is in regulation of technical data associated with defense articles. Moreover, our understanding is that DDTC does not intend to use this note to control technical data pertaining to general use commodities, even if there is knowledge of which general use commodity it will be used with (*i.e.*, a “particular commodity”).

Second, the recommended change reconciles Note 3, paragraph 5 with Note 3, paragraph 4. Paragraph 4 excepts technical data that was, or is being, developed with knowledge that it is for use in or with both defense articles and commodities not on the U.S. Munitions List. Without some revision along the lines suggested here, paragraphs 5 could be read to carve out technical data that was developed with knowledge that it would be used with both defense articles and non-defense articles, while controlling technical data developed without knowledge that it would be used with a defense article. This does not appear to be consistent with the DDTC’s concern for regulating defense articles.

Third, the recommended substitution harmonizes the Note 3 with the corresponding proposed revisions to the EAR set forth in the BIS Proposed Rule relating to the proposed definition for the term “peculiarly responsible” in proposed revisions to proposed EAR § 772.1. Specifically, the BIS Proposed Rule carves out of the definition of “Peculiarly responsible” various scenarios, including when an item “was or is being developed with ‘knowledge’ that it would be for use in or with commodities or software described in . . . an ECCN controlled for AT-only reasons and also EAR99 commodities or software....” (proposed EAR § 772.1, “Peculiarly responsible, subparagraph (6).) Commodities or software falling under ECCNs controlled for reasons only of AT or under EAR99 are under less restrictive export controls than other items that are “peculiarly responsible” for achieving controlled performance levels. Our proposed recommendation relating to ITAR § 120.46, Note 3, paragraph 5 would render the proposed term “required” consistent with the proposed EAR definition of “peculiarly responsible” in this respect.

B. ITAR § 120.41

We note that the proposed definition of “required” tracks with the ITAR’s existing definition of “specially designed” (*see* ITAR § 120.41), and that the existing definition of “specially designed” contains similarly unclear language in paragraph (b)(5), referring to “a

particular commodity (e.g., a F/A-18) or type of commodity (e.g., an aircraft or machine tool)” when “a particular defense article (e.g., a F/A-18 or HMMWV) or type of defense article (e.g., an aircraft or machine tool).” It does not appear that there was any discussion of this aspect of the definition of “specially designed” in the promulgation of CEECR 120.41. *See* 78 Fed. Reg. 22747 (Apr. 16, 2013). As such, we recommend that DDTC also revise the definition of “specially designed” to substitute the words “particular defense article” for “particular commodity” and “type of defense article” for “type of commodity in ITAR § 120.41(b)(5).

VIII. Proposed ITAR § 120.9 – “Defense Service”

Under DDTC’s Proposed Rule, proposed ITAR § 120.9(a)(2) and its corresponding note provide:

(2) The furnishing of assistance (including training) to a foreign person (see § 120.16), whether in the United States or abroad, in the development of a defense article, or the integration of a defense article with any other item regardless of whether that item is subject to the ITAR or technical data is used;

Note to paragraph (a)(2): “Integration” means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software to enable operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from “installation.” Installation means the act of putting an item in its predetermined place without the use of technical data or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). The “fit” of an item is defined by its ability to physically interface or connect with or become an integral part of another item.

80 Fed. Reg. at 31534 (emphasis added to highlight text of particular concern).

Having reviewed the text of proposed ITAR § 120.9(a)(2) and the note thereto, as well as DDTC’s responses to prior comments, we believe that DDTC’s conditioning the term “installation” on there being “no use of technical data” is overbroad and could have significant negative consequences across a number of industries. As discussed below, we believe the proposed text of the Note has a number of drawbacks.

Inconsistency Between Section 120.9(a)(2) and its Note. To begin with, there is inconsistency between proposed ITAR § 120.9(a)(2) and its Note. The proposed text of Section 120.9(a)(2) defines “defense service” “*regardless of whether . . . technical data is used.*” The corresponding note, however, then makes the use of *any* technical data dispositive with regard to whether the service will be treated as “integration” rather than merely “installation” – apparently even when limited to “fit.” Thus, the proposed rule and note read in conjunction are internally

inconsistent because, as proposed, the determination of whether a defense service is rendered is not without regard to the use of technical data.

Receipt / Use of Technical Data is Common and Often Necessary When Specially Designing Components for Defense Articles. In addition, proposed ITAR § 120.9(a)(2) and its Note fail to recognize that the receipt and use of technical data is common and often necessary when specially designing components for defense articles. In the automotive, aerospace, and maritime sectors, for example, it is common for defense contractors manufacturing military platforms or their subsystems to contract with commercial suppliers for specific parts and components. As is commonly known, the form factor of these parts and components often must be modified in a variety of ways to fit the vehicle or aircraft, or an assembly thereof. Indeed, the transfer of jurisdiction from DDTC to BIS over such “600 Series” items expressly acknowledges this issue and has been a major goal and achievement of the ECRI.

As part of the process of developing, modifying, and manufacturing commercial items specially designed for use in defense articles, it is common and often necessary (though not always the case) that the manufacturer of the platform will provide certain technical data regarding the vehicle so the commercial component supplier can make appropriate modifications to the component to ensure that the form factor of the component will allow it to “fit” the vehicle – i.e., to physically interface or connect with or become an integral part of another item.

Which technical data is shared with the component manufacturer is determined by the vehicle manufacturer. In some cases, the vehicle manufacturer will provide very limited technical data regarding only those vehicle systems into which the component must fit. In other cases, the vehicle manufacturer might provide a broader range of data about the vehicle. In relatively few cases, however, would a defense contractor provide no technical data to component manufacturers that are specially designing components for a defense article.

Our concern, therefore, is that registration as a manufacturer / exporter under the ITAR and obtaining a Technical Assistance Agreement or other authorization under the ITAR would be required in many (or even most cases) merely to modify a commercial item for installation into a defense article – in addition to obtaining BIS authorization for export of the item.

Proposed Rule Threatens to Undercut ECR By Requiring DDTC and BIS Licenses for 600 Series Items. Moreover, as written, proposed ITAR § 120.9(a)(2) and its Note threaten to undercut the ECRI by in effect requiring both DDTC and BIS licenses for 600 Series Items. This potential dual licensing (and registration) requirement is inconsistent with and threatens to undercut what is a hallmark of the President’s ECRI. With due respect to differing perspectives, if the intent were to transfer control over specially designed components of defense articles to BIS but continue to regulate under the ITAR the process of component design and manufacture, the very rationale of the reform is called into question from the standpoint of industry. In short, we would urge great care in not allowing an (unintentionally) overbroad explanation of “integration” to gut the significant and welcome efficiencies that the ECRI has promised and can achieve. We note further that any such dual licensing is likely to be identified by foreign customers who will seek foreign sources of supply to “engineer around the ITAR.”

Modification / Engineering Analysis of the Defense Article *Beyond* Component “Fit” Is a More Reasonable Basis for Control under section 120.9(a)(2), Not Whether Technical Data was Provided or Relied Upon When Specially Designing the Component. Modification/engineering analysis of the defense article *beyond* component “fit” is a more reasonable basis for control under proposed ITAR § 120.9(a)(2), not whether technical data was provided or relied upon when specially designing the component. Whether a defense service is deemed to be exported would be more reasonably and objectively determined by the nature of the engineering analysis or “integration” provided to the foreign recipient (*i.e.*, the service), not the technical data provided to or relied upon by the component manufacturer specially designing a commercial item for “installation” into the defense article. We understand DDTC’s interest in asserting control over major modifications to the military platform *beyond* “fit.” For the reasons set forth above, however, we do not believe that modifications limited to “fit” – regardless of whether technical data is used – should be controlled as a defense service.

Introduction of Software Must Be “Required” for the Operation of a Defense Article to Constitute A Defense Service. On a separate but related issue, the CEECR has concerns regarding DDTC’s proposal to include in the definition of “integration” for purposes of the Note the following text: “*Integration includes the introduction of software to enable operation of a defense article....*” The language as proposed is significantly overbroad and should be revised.

Numerous examples come to mind where introducing or installing software on a defense article should not be controlled as a defense service – e.g., installing a commercial operating system (such as Windows 10) on a Category XI defense article. The CEECR believes it would be more appropriate to base the control of software introduction on whether the software introduced and/or some unique feature of the installation itself is “required” for operation of the defense article.

We recommend that the introduction of the software must be “required” – *i.e.*, “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions.” Using such a defined term also is preferable to the undefined term “enable” in that it furthers the goal of consistency of interpretation across sections of the ITAR and the EAR.

As discussed above under Part VII, the CEECR believes that DDTC and BIS should omit the “catch and release” definition of “peculiarly responsible” and allow exporters to continue to rely on the dictionary definitions of “peculiarly responsible.” Moreover, we urge DDTC to revise the proposed definition of “required” in the ways discussed above under Part VII.

DDTC Should Harmonize Proposed ITAR §§ 120.9(a)(1) & (a)(2) to Preserve Distinction Between Installation and Integration. In its response to comments on the prior proposed rules regarding ITAR §120.9, DDTC writes:

The modifications of the “defense article” to accommodate the fit of the item to be integrated, which are within the activity covered by installation, are only those modifications to the “defense article” that allow the item to be placed in its predetermined location. Any modifications to the design of a “defense article” are beyond the scope of installation. Additionally, while minor modifications may be made to a “defense article” without the activity being controlled under (a)(2)

as an integration activity, all modifications of defense articles, regardless of sophistication, are activities controlled under (a)(1) if performed by someone with prior knowledge of U.S.-origin “technical data.”

80 Fed. Reg. at 31531 (emphasis added to highlight text of particular concern).

If DDTC intends to accept any of CEECR’s comments and suggested revisions to ITAR §120.9(a)(2), then some harmonization is required to resolve the apparent trumping of subsection (a)(2) by (a)(1), if the person performing the installation has prior knowledge of U.S.-origin technical data. We believe this could be accomplished with additional clarifying language in the Note to subsection (a)(2) and have suggested this below.

In addition to our concerns about the impact on subsection (a)(2), the CEECR believes that DDTC’s defining whether a defense service is rendered by virtue of whether an engineer has knowledge of technical data is again overbroad. While we appreciate DDTC’s attempts to limit in certain respects what type of technical data an engineer might have in her head that would rise to the level of performing a defense service (e.g., technical data related to the same USML category as the current project), we believe it remains overbroad and not as well defined as industry would hope.

Under the current proposed rule, an engineer who had prior knowledge of technical data in Category XI could not perform any modification related to another Category XI item (even mere installation) without having rendered a defense service. We need not remind you how broad certain categories of the USML remain even after ECRI. We believe a more logical approach would be break the defense service analysis into elements to look at several factors to determine whether a defense service had been rendered, including for example, (1) knowledge and (2) use of (3) U.S.-origin (4) technical data (5) “required” (6) to modify (among other types of activities) (7) a defense article (8) beyond “installation” / “fit.”

We do not mean to suggest that this is a perfect alternate formulation, but it illustrates that the issue contains more facets than an engineer’s knowledge of technical data, which would benefit from a more refined rule. We note that the proposed revision to the Note to proposed subsection (a)(2) below does not alleviate this broader concern with (a)(1). It should, however, reconcile the tension between the two provisions.

Proposed Revision. For the reasons discussed above, the CEECR recommends that DDTC revise the Note to paragraph (a)(2) of proposed ITAR § 120.9 as follows (deletions are indicated with strike-throughs and additions are in small caps):

Note to paragraph (a)(2): “Integration” means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software ~~to enable~~ “required” for operation of a defense article, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Integration is distinct from “installation.” Installation means the act of putting an item in its predetermined place without ~~the~~

~~use of technical data~~ or any modifications to the defense article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, ~~and there is no use of technical data~~). The “fit” of an item is defined by its ability to physically interface or connect with or become an integral part of another item. ([S]ee § 120.41). *A TRANSFER OF TECHNICAL DATA OR OTHERWISE HAVING KNOWLEDGE OF TECHNICAL DATA RELATED TO “FIT” OR PROVIDED FOR THE PURPOSE OF ACCOMMODATING THE “FIT” OF AN ITEM IN A DEFENSE ARTICLE IS NOT ITSELF SUFFICIENT TO ESTABLISH “INTEGRATION” (E.G., LIGHT ARMORED VEHICLE MANUFACTURER PROVIDES A STEERING COLUMN MANUFACTURER TECHNICAL DATA REGARDING THE VEHICLE OR ITS SUBSYSTEMS TO ENABLE MODIFICATIONS TO A COMMERCIAL STEERING COLUMN, BUT NO TECHNICAL DATA RELATED TO MODIFICATIONS TO THE VEHICLE (OTHER THAN TO ACCOMMODATE THE FIT OF THE STEERING COLUMN) ARE TRANSFERRED FROM THE STEERING COLUMN MANUFACTURER TO THE VEHICLE MANUFACTURER).*

We believe that the suggested revisions above, including the addition of the last sentence, would be a reasonable solution to accommodate industry’s concerns – yet still safeguard national security interests.

Manufacturing and Production Consulting Services. U.S. persons that are consultants in specialized manufacturing and production optimization processes and techniques, such as Six Sigma and Lean Manufacturing, are often asked by foreign manufacturers of defense articles to provide consulting services in this area. The current definition of "defense services" is so broad that such services are captured when the services are associated with the manufacture or production of foreign defense articles.

While the proposed changes to ITAR § 120.9(a)(1) removes the term "manufacture" from the current definition and adds language attempting to limit the scope of "assistance" considered to be a defense services, the proposed definition may still unintentionally capture Six Sigma or Lean Manufacturing techniques associated with the production of a foreign defense article. For example, it is possible that a U.S. person who may have obtained some "knowledge of U.S. origin technical data directly related to the defense article that is subject to the assistance, prior to the performing of the service" in the foreign country. However, the mere knowledge of ITAR controlled technical data should not be sufficient to capture a production-related consulting service if the information conveyed is general in nature and does not change the technical specifications or military characteristics of a foreign defense article. For example, a U.S. person consultant may provide guidance to a foreign defense article manufacturer on how to optimize workflows of a production line used to manufacture defense articles. Similarly, a U.S. person consultant may recommend the use of a particular commercial-off-the-shelf adhesive in lieu of the current one being used. In both cases, the services provided should not be considered a defense service.

As a result, we recommend that an additional note to paragraph (a) be included as an example of an activity that is not a defense service:

10. The furnishing of consulting services to a foreign person in the production of a foreign defense article, such as Six Sigma or Lean Manufacturing techniques, as long as the information conveyed does not rely on U.S. origin technical data and does not change the technical specifications or military characteristics of a foreign defense article.

Absence of Comments on Other Aspects of Proposed ITAR § 120.9 Should Not Be Viewed as CEECR's Endorsement of Those Subsections. These comments primarily address certain elements of proposed ITAR § 120.9(a)(2) and its Note. We urge DDTC, however, not to infer from the lack of comments on other aspects of the rule that the CEECR endorses the rest of the proposed rule. While this version of proposed ITAR § 120.9 represents a significant improvement over prior proposed rules on defense services, the CEECR believes additional thought should be dedicated to this section in particular, given the complexities associated with controlling defense services. We would be happy to present additional comments to DDTC regarding other concerns and opportunities for improvement of the proposed rule.

IX. "Public Domain" Under the DDTC Proposed Rule

A. Public Domain-Related Assertions Relevant to Proposed ITAR § 120.11

In the preamble to the DDTC Proposed Rule, DDTC asserts that a requirement to obtain prior approval from DDTC or certain other U.S. Government agencies or officials before technical data can be deemed to be in the public domain, even if it has already been released to the public, is not a new requirement and is actually a currently existing requirement. The CEECR disagrees with this assertion and urges DDTC to revisit the history of this issue, and reconsider the proposed definition of Public Domain.

As an initial matter, it is important to note that a previously written prior approval requirement under the ITAR was repealed in 1984 due to First Amendment concerns. These concerns were expressed to DDTC by the Department of Justice on three occasions in 1978, 1981 and 1984. In addition, in 1981, the U.S. Congress recommended to the State Department that the ITAR be revised to avoid First Amendment issues.

Additionally, in a review of court cases involving the Arms Export Control Act since that time, DDTC has not asserted a prior approval requirement to put information into the public domain. In one case from 1996 that is directly tied to this discussion, an exporter in 1994 filed two commodity jurisdiction (CJ) requests. *See Karn v. Dep't. of State*, 925 F. Supp. 1 (D.D.C. 1996). In the first request, the exporter requested a determination of a textbook that concerned cryptography. The textbook included source code in print and on a diskette in an electronic text file. The second CJ request held that the source code on the diskette was ITAR-controlled software even though it was the identical source code that was printed in the textbook.

Of importance here, even though the textbook in *Karn* admittedly contained information required for the design, development, assembly, and manufacture of a defense article (*i.e.*,

technical data), DDTC held that the textbook was in the public domain. However, the textbook was published prior to the CJ determination. There is no evidence that indicates prior approval from the author or publisher of this textbook to place it into the public domain was sought or granted by DDTC. Similar to all the “technical data” published in other textbooks, journals, conferences, open meetings and on the Internet, it is doubtful that prior approval to publish the textbook was sought or required by DDTC. If it believed that prior approval was required to publish the book, DDTC did not articulate that view or, apparently, take steps to enforce it.

Since that court case, we are unaware of any other publicly known claim from DDTC that there is a prior approval requirement to put information into the public domain. Even in the ongoing litigation in *Defense Distributed v. Dep’t. of State*,⁷ DDTC has taken the position that “the regulations . . . carve out a wide exemption for ‘public domain’ data that helps ensure [the ITAR’s] reach is appropriately limited. . . . For this reason, there is simply no substantial overbreadth here.” Government Brief in Opposition at 22 (June 10, 2015).

While we note, that as a legal matter, the definition of public domain relates to an exclusion from the scope of the ITAR rather than an exemption from an otherwise subject ITAR requirement, even DDTC admits in federal court that without a public domain exclusion there would be constitutional issues under the First Amendment. If DDTC’s position is that there is a prior approval requirement to use an exclusion, then there is no public domain exclusion at all.

In addition, the CEECR notes with concern that DDTC’s assertion of a prior approval requirement to use the public domain exclusion provided in the definition of “technical data” in ITAR § 120.10(b) means that fundamental research performed by the academic and scientific community at accredited institutions of higher learning in the United States requires prior approval from the U.S. Government. It is difficult to imagine a scenario where DDTC’s asserted prior approval requirement on academic and scientific speech by the university community would survive First Amendment scrutiny.

For all of the reasons discussed above, the CEECR urges DDTC revisit the history of this issue, and reconsider the proposed definition of Public Domain and confirm there is no existing prior approval requirement.

B. Proposed ITAR § 120.11(b)

It is the CEECR’s view that proposed ITAR § 120.11(b), which relates to the prior approval requirement to put information into the public domain discussed above, would amount to an unconstitutional prior restraint. Moreover, even if the provisions set forth in proposed

⁷ While we have knowledge of this court case and DDTC’s May 8, 2013 letter to Defense Distributed that implies a prior approval requirement, we note that this is legally insufficient to serve as legally recognized public notice. DDTC’s private letter to Defense Distributed was not made public by DDTC but by Defense Distributed. Further, we only have knowledge of the lawsuit that was filed in 2015, because it was brought by Defense Distributed. DDTC has taken no action itself to make its material interpretation of the law known to the public.

ITAR § 120.11(b) were content-neutral, the First Amendment still requires that the U.S. Government establish specific procedural safeguards, and as written, the prior approval requirement lacks such constitutionally required procedural safeguards. Accordingly, the CEECR urges DDTC not to include proposed ITAR § 120.11(b) when issuing the final rule.

The procedural safeguards required under the First Amendment to impose a lawful prior restraint are: “(1) any restraint prior to judicial review can be imposed only for a specified brief period during which the status quo must be maintained; (2) expeditious judicial review of that decision must be available; and (3) the censor must bear the burden of going to court to suppress the speech and must bear the burden of proof once in court.” *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 227-228 (1990).

Here, the ITAR expressly exempts judicial review of approval and licensing decisions in ITAR § 128.1, and it concedes that it is a “highly discretionary” system. Further, there are no strict timelines for a licensing or approval determination to be made. Additionally, there is added delay in receiving an approval because of the required Congressional notification under Section 38(f) of the Arms Export Control Act. The AECA also expressly prohibits judicial review of designations of items as on the U.S. Munitions List.

Significantly, a federal court already has held that key aspects of the ITAR were an unconstitutional prior restraint that failed to provide any procedural safeguards. *See Bernstein v. Dep’t. of State*, 945 F. Supp 1279, 1289 (N.D. Cal. 1996). In that case, the court stated that “[t]he ITAR scheme, a paradigm of standardless discretion, fails on every count, and further noted that “[t]his court finds nothing in the ITAR that places even minimal discretion of the licensor and hence nothing to alleviate the danger of arbitrary or discriminatory licensing decisions.” *Id.* at 1286. The federal court even drew attention to DDTC ignoring a discussion on procedural safeguards in defending the lawsuit. *Id.* at 1286 (“[DDTC’s] arguments . . . are notable for the conspicuous absence of discussion of the prior restraint doctrine”).

In light of the above precedent, and considering that proposed ITAR § 120.11(b) does not provide the constitutionally required safeguards, the CEECR urges DDTC not to include proposed ITAR § 120.11(b) when issuing the final rule.

C. Proposed ITAR § 120.11 – Note 1

Note 1 to proposed ITAR § 120.11 makes no distinction between public domain and restricted information, and as such, it can be read to require government authorization before publishing, disseminating, or exporting any and all information. This is an undue burden that would require submission to the U.S. Government of every journal article, speech, book, and manuscript prior to any attempts to publish them. It would put undue liability on anyone who receives such potential information as requiring proof that consent from the government was obtained in order to publish said information, and there is no format or methodology given for obtaining this consent. For all of these reasons, the CEECR recommends that DDTC not include Note 1 to proposed ITAR § 120.11 when issuing the final rule.

D. Proposed ITAR § 120.6(b)(3)(iii)

Proposed ITAR § 120.6(b)(3)(iii) states that items that “concern general scientific, mathematical, or engineering principles commonly taught in schools . . .” are not defense articles subject to the ITAR. The CEECR requests that the word “general” be deleted as it is not defined and could limit what is covered to only entry-level courses as opposed to a broad range of scientific instruction.

Significantly, courts have held that only information “significantly and directly related to defense articles” are subject to the ITAR. *See United States v. Edler Industries*, 579 F. 2d 516 (9th Cir. 1978). It is hard to imagine that any scientific, mathematical, or engineering principles *commonly* taught in schools is “significantly and directly related to” a defense article. Thus, by only excluding “general” information that is *commonly* taught in this academic context rather than any information *commonly* taught in this academic context, proposed ITAR § 120.6(b)(iii) fails to follow the holding of *Edler*.

DDTC is already on the public record that it maintains such a narrow construction:

In recent years, some parts of the academic community have expressed concern about the application of government export regulations to disclosures of information in university classrooms. This concern (for example, that the language of the ITAR was overly broad) did not occur because of any changes in the text of the ITAR, or in the policies and practices of the Department of State in administering the regulations. In order to address the concerns expressed about the regulations, however, the language with regard to what information is subject to ITAR controls has been clarified. The Department's long-standing practice of regulating only information that is directly related to defense articles, as reflected in *U.S. v. Edler*, 579 F. 2d 516 (9th Cir. 1978), remains unchanged. *See* 49 Fed. Reg. 47,683 (Dec. 6, 1984).

For all of the reasons discussed above, the CEECR urges DDTC to delete the word “general” from proposed ITAR § 120.6(b)(iii) in accordance with DDTC’s long-standing adherence to only controlling technical data that is significant and directly related to a defense article.

In addition, the CEECR notes that the lack of a definition of the term “directly related” under the ITAR is problematic. As a matter of law, the AECA only provides the legal authority to control defense services (as defined by ITAR § 120.9), software (as defined by ITAR § 120.45), and technical data (as defined by ITAR § 120.10) that are directly related to a defense article. Therefore, defense services, software, or technical data that are not “directly related” to a defense article are not controlled on the USML, and items not controlled on the USML are not subject to the statutory authorities under the AECA. As such, the “directly related” requirement is a material qualifier. The ABA further notes that the only control criteria on software is for software directly related to a defense article, which in the absence of a definition will result in different understandings within government and industry.

Although DDTC is now proposing a definition of “required” under proposed ITAR § 120.46, the CEECR notes that the AECA is limited to only controlling defense services, software and technical data that are “significant and directly related to defense articles” as required by the narrowing construction in *United States v. Edler*. While DDTC is satisfying the first limitation with a definition of “required,” it is not defining the second limitation of what “directly related” means. Further, as proposed, there would be no means to know what constitutes software “directly related” to a defense article.

For all of these reasons, the CEECR recommends that the meaning of “directly related” be defined by DDTC to ensure common understanding within industry and the government as to what constitutes a defense service, technical data, or software that is “directly related” to a defense article.

E. Proposed ITAR § 120.47 and Proposed ITAR § 120.49

The proposed definition of “development” in proposed ITAR § 120.47 and its distinction from “fundamental research” under proposed ITAR § 120.49(c) needlessly restricts research. “Fundamental research” often involves activities included in the proposed definition of “development” such as design research, design analysis, and testing of prototypes to conclude whether a hypothesis being tested is correct. For example, it is often necessary to build some sort of prototype to determine if calculations in engineering and mathematics match a real-world application. Such activities should not be considered “development” since they are simply forms of testing that many research institutions perform. In view of this fact, the CEECR urges that such activities should be stricken from the definition of “development” in proposed ITAR § 120.47.

The definition of “fundamental research” under proposed ITAR § 120.49(c) includes the phrase “this is distinguished from . . . industrial development.” The term “industrial” is not defined, but if it is taken as the definition of “development” in proposed ITAR § 120.47, such interpretation could lead to unintended consequences, such as potentially hampering the advancement of science and technology being made at universities. Also, such interpretation would conflict with proposed ITAR § 120.49(c)(2)(ii) (*Applied Research* definition), which includes the effort that, in part, “attempts to determine and exploit potential scientific discoveries . . .,” because an amount of development is often required to ensure that sound theories and good ideas can be put into practice. As such, the CEECR urges that DDTC strike the word “development” from proposed ITAR § 120.49(c) and expand the definition of “applied research” under proposed ITAR § 120.49(c)(2) to include development within the context of fundamental research that is intended for publication.

X. “Fundamental Research” Under the BIS Proposed Rule

A. Proposed EAR § 734.3(b)(3)(iii)

Proposed EAR § 734.3(b)(3)(iii) states that information and software that “concern general scientific, mathematical, or engineering principles commonly taught in schools . . .” are not subject to the EAR. For the same reasons discussed above under CEECR VII.D, the CEECR

urges that the word “general” be deleted from proposed EAR § 734.3(b)(iii) since that word is not defined and could limit what is covered to only entry-level courses as opposed to a broad range of scientific instruction.

B. Proposed EAR § 734.8(b) – Note 2

Proposed revised EAR § 734.8 concerns technology that arises during, or results from, fundamental research, and excludes certain such technology from the scope of the EAR if certain conditions are met (e.g., intended to be published). As written, Proposed Note 2 to paragraph (b) could cause a requirement to renegotiate many government contracts held with universities and any companies that engage in fundamental research in an attempt to remove the clause lest the status of research as fundamental be challenged, creating unnecessary and undue burdens on researchers.

In contrast, proposed Note 2 to proposed ITAR § 120.49(b) is preferable to Proposed Note 2 to proposed EAR § 734.8(b). Proposed Note 2 to proposed ITAR § 120.49(b) states: “Research that is voluntarily subject to U.S. government prepublication review is considered intended to be published for all releases consistent with any resulting controls.” This is interpreted to mean that prepublication review does not necessarily impede a fundamental research designation.

For all of the reasons discussed above, and to promote consistency between the ITAR and the EAR, the CEECR recommends that the same or similar language to that contained in proposed Note 2 to proposed ITAR § 120.49(b) be used in Proposed Note 2 to proposed EAR § 734.8(b).

C. Proposed EAR § 734.8(c)

Proposed EAR § 734.8 does not explicitly state that software resulting from fundamental research is “not subject to the EAR.” This is in stark contrast to the way in which software is treated under current EAR § 734.8. The CEECR proposes that language should be added to Proposed EAR § 734.8 that explicitly states that software resulting from fundamental research is “not subject to EAR.”

Another key concept from existing EAR § 734.8 also is omitted from proposed EAR § 734.8. Specifically, current EAR § 734.8(b)(1) contains the phrase “research conducted by scientists, engineers, or students at a university normally will be considered fundamental research,” but proposed EAR § 734.8(c) is missing this phrase. The CEECR recommends that this language from current EAR § 734.8(b)(1) be included in proposed EAR § 734.8(c). We believe that this wording should be carried to the proposed rules to make clear what is covered.

XI. Issues Relating to the BIS May 20, 2015 Wassenaar Arrangement Implementation Rule Proposed Rule

A. Timing of Final Rule Implementation

If the effective date for the final rule relating to the Wassenaar Arrangement Implementation Rule is scheduled to be on or shortly after the final rule's publication date, the CEECR believes that there are serious risks that such an abrupt start to the rule will disrupt existing contracts for "cybersecurity items" and will put the parties thereto in immediate non-compliance with the rule. As explained below, the CEECR recommends that BIS establish the effective date of the final rule to be *at least six months* later than the final rule's publication date.

As proposed, the Wassenaar Arrangement Implementation Rule will apply to an unknown and potentially large number of items "not previously designated for export control." In the preamble to the May 20 Proposed Rule, BIS acknowledges that the new *cybersecurity controls* will apply export controls, and impose license requirements, on items not previously controlled by the EAR or items that previously were eligible for License Exception ENC. As BIS explains:

"Although these cybersecurity capabilities⁸ **were not previously designated for export control**, many of these items have been controlled for their 'information security' functionality, including encryption and cryptanalysis."⁹

However, neither the preamble nor the proposed rule itself addresses how BIS will bring the final rule into effect (*i.e.*, whether the publication date of the final rule will be the same as its effective date).

⁸ The "cybersecurity capabilities" refers to preceding sentences where BIS identifies the following as "cybersecurity items":

- "systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software";
- "software specially designed or modified for the development or production of such systems, equipment, or components";
- "software specially designed for the generation, operation or delivery of, or communication with, intrusion software";
- "technology required for the development of intrusion software";
- "Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor"; and
- "development and production software and technology therefor".

See 80 Fed. Reg. at 28853 (emphases added).

⁹ *See id.*

On May 20, 2015, when BIS issued the Wassenaar Arrangement Implementation Rule, many U.S. firms may have been under contract (and perhaps multiple contracts) to export, reexport or transfer “cybersecurity items” that had not previously been designated for export control. Similarly, universities conducting “fundamental research” and development of technologies for commercialization will probably have had ongoing faculty/student research teams engaged in activities that, under the final rule, may constitute the export, reexport or transfer of “cybersecurity capabilities” not previously designated for export control.

Furthermore, between the proposal date and the final rule’s publication date, additional U.S. persons will probably have entered into such contracts or will soon do so, especially in light of the fact that there has not been extensive media reportage about the proposed rule. Numerous U.S. persons that transact in “cybersecurity items” are probably still unaware of the proposed rule, and even those aware of it may not have been briefed by counsel on the compliance obligations that will arise when the rule is adopted and comes into effect.

If the final rule becomes effective immediately, many “U.S. persons”, as defined in Section 772.1 of the EAR, will be at risk of failing to comply with the final rule when it comes into effect. We think such noncompliance will be the result for several reasons.

First, U.S. persons will have pre-existing contractual obligations to export, reexport or transfer “cybersecurity items” that will be newly designated for export control and subject to license requirements. Many such persons may have little, if any, awareness of the proposed rule and be unaware of the risks that the final rule may pose to their existing and contemplated contracts for “cybersecurity items” or to their internal research and development programs involving “cybersecurity items.”

With respect to contracts for “cybersecurity items” that will not, by their own terms, terminate before the final rule’s effective date (“Subject Contracts”), certain U.S. parties to these Subject Contracts will find themselves in a double-bind on the effective date: immediate compliance with the rule will require them to take actions that may, when taken, put them in material breach of the relevant Subject Contracts.

Parties to Subject Contracts (and their officers and directors) who are unaware of the proposed rule or unaware of the compliance obligations that the final rule will impose on their enterprises and dealings will have had no reason or opportunity to negotiate and structure such contracts in order to avert the double-bind of duties to comply with the final rule and obligations to complete performance of their Subject Contracts.

Few, if any, of the existing Subject Contracts are likely to contain provisions that condition the parties’ export, reexport or transfer obligations on compliance with the final rule. Moreover, the scope and terms of the final rule may differ substantively in crucial details from the proposed rule. As a result, until the final rule is published by BIS, the officers and directors of such enterprises engaged in Subject Contracts will have no reliable knowledge of the final rule’s scope and terms. Without knowledge of the precise scope and terms of the final rule, it is not practicable for parties to Subject Contracts to negotiate provisions to address that rule. For

the same reasons, counsel cannot competently advise clients on ways to address the yet-to-be disclosed version of the final rule in a Subject Contract.

Boilerplate provisions in commercial contracts might mitigate some of the transactional risks, but will probably not adequately address them or control them within the limits of a corporate client's tolerance of risks. A typical boilerplate provision that obligates all parties to a contract to "comply with all applicable U.S. export control laws and regulations", if included in a Subject Contract, would probably not avert the risks posed by the final rule coming into effect on or very soon after its date of publication by BIS. Similarly, a typical *force majeure* or event of excusable delay clause will not sufficiently reduce such risks, particularly in states (such as New York) whose courts tend to construe *force majeure* clauses narrowly.

Second, the final rule will impose broad licensing obligations on the export, reexport or transfer of "cybersecurity items" that were previously designated as EAR 99 or eligible for License Exception ENC. As a result, and because there are no license exceptions for intracompany transfers, end users or end uses, or deemed exports,¹⁰ many U.S. companies and research organizations will be required to obtain licenses to be in compliance with the final rule as of its effective date. However, prior to the publication of the final rule, it will not be possible for U.S. persons affected by the rule to identify with certainty all the instances in which a license will be required.

Moreover, once the final rule is published, U.S. persons who engage in exports of "cybersecurity items" will need to spend considerable time and resources to identify situations in which licenses are required as well as prepare, submit and receive such licenses. In order to obtain the necessary licenses, there must be ample time between the publication of the final rule and its effective date to allow U.S. persons to assess the need for, apply for and receive the licenses required under the final rule. For companies that engage in exports of, or that design and develop "cybersecurity items" (and whose engineering staff may include foreign nationals), there may be a need to apply for and obtain multiple licenses. Without sufficient time to do so after the final rule is published, such companies will be unable to comply with applicable license requirements without bringing certain aspects of their business organization to a halt. This, of course, could disrupt contractual relationships and impose financial hardship, especially on small businesses.

As discussed above, the less time there is between the publication of the final rule and its effective date, the greater will be the risk that U.S. persons affected by the final rule will be abruptly and detrimentally confronted by their duties to comply with the final rule and their commitments to complete existing contractual obligations or ongoing research programs.

The CEECR respectfully recommends that BIS establish the effective date of the final rule to be *at least six months* later than the final rule's publication date.

¹⁰ See BIS's FAQs on Intrusion and Surveillance Items posted by BIS at <http://www.bis.doc.gov/index.php/policy-guidance/faqs>.

A minimum of a six-month interval between publication and effective date is necessary in order for there to be sufficient time to come into compliance with the final rule. During this interval, we expect the following activities to occur:

1. U.S. persons impacted by the rule will be briefed by counsel on the scope, terms, and significance of the final rule;
2. Counsel and compliance officers will advise clients on compliance duties under the final rule, the risks of non-compliance, and the appropriate changes to export compliance programs, including training, an activity that will require significant time due to the proposed rule's complexity;
3. U.S. persons impacted by the rule will review existing and contemplated Subject Contracts to identify which existing contractual obligations may conflict with compliance obligations under the final rule and take appropriate actions, such as negotiating and executing amendments to existing Subject Contracts to avert the risk of non-compliance with the final rule while, at the same time, fulfilling contractual obligations; and
4. U.S. persons impacted by the rule will survey their business or research operations to identify the need for licenses and, if needed, will prepare, submit and wait to receive such licenses.

The CEECR believes that a six-month delay, at a minimum, between the publication date of the final rule and its effective date is necessary for U.S. persons affected by the rule to comply with their obligations under the final rule without undue hardship and the risk of substantial disruption to their business and research operations.

B. Obligations Prior to the Effective Date

The CEECR believes that companies and their counsel will be concerned about the obligations that U.S. persons may have for “cybersecurity items” that they exported, reexported, or transferred prior to the effective date of the final rule.

In particular, they will need to know the legal status of “cybersecurity items” not previously designated for export control that foreign nationals received or gained access to before adoption of the final rule. Similarly, they will need to know whether pre-rule “deemed exports” of such “cybersecurity items” trigger any obligations by the exporter to recapture or recover such items from the foreign national recipients.

The CEECR recommends that BIS consider issuing guidance (perhaps in the form of additional FAQs) that would address the status of pre-rule exported “cybersecurity items” and the compliance duties of exporters and recipients of such items – where such items have not previously been designated for export control.

C. Exporter's Knowledge

In the preamble to the May 20 Proposed Rule, it states that the “EAR also prohibits the export of equipment if the exporter intends it will be combined with other equipment to comprise a system described in the new entry.” 80 Fed. Reg. at 28854 (emphasis added). While this statement suggests that only the exporter’s intent matters, elsewhere in the proposed rule, it indicates that violations also can result from what the exporter knows that the recipient intends to do with the item. For example, in the proposed text for revisions to ECCN 5A001 (at 80 Fed. Reg. 28661), the language reads:

“[S]uch equipment may not be sold separately **with knowledge** that it will be combined with other equipment to comprise a system described in the new paragraph.” (Emphasis added.)

This language makes clear that the exporter’s “knowledge” is the key factor.

It is the CEECR’s belief that emphasis on an exporter’s knowledge” is consistent with an exporter’s duty to determine if the export recipient or end-user intends to make prohibited or unlicensed use of the controlled item and should be emphasized by BIS. Accordingly, assuming that this view of the CEECR is accurate, the CEECR recommends that BIS clarify (in the preamble to any final rule that is issued) that an exporter’s knowledge is critical to determining whether a violation may or may not have occurred if an export recipient or end-user combines an item with other equipment to comprise a new controlled system.

D. Proposed EAR § 742.6(b)(5)

Proposed EAR 742.6(b)(5) defines “foreign commercial partner” to mean:

a foreign-based non-governmental end-user that has a **business need** to **share** the proprietary information of the U.S. company and is **contractually bound** to the U.S. company (*e.g.*, has an established pattern of continuing or recurring contractual relations).

80 Fed. Reg. 28858 (emphasis added). As discussed below, the CEECR is concerned that each of the three underlined terms in the above definition could encourage export practices that are not intended by BIS and that would be contrary to the objectives of the EAR.

The term “**business need**” is not defined in the May 20 Proposed Rule or elsewhere in the EAR. Every activity of a business can be characterized as a “business need” when its owners or operators perceive an apparent benefit to doing so. In fact, there is little that a company cannot characterize as a “business need” if doing so will benefit the company. As a result, the term “business need” may be interpreted by exporters and export recipients so expansively as to render it applicable to almost any activity of a business. Such interpretations could easily reduce to a meaningless and thus irrelevant term an otherwise important requirement for an export recipient to qualify as a “foreign business partner.” Exporters would be encouraged to accept any claim of a “business need” by the prospective end-user.

There appears to be an error in using the verb “**to share**” as the operative term in the requirement that an end-user have “a business need to “**share**” the proprietary information of the U.S. company.” As used in that context, “**share**” conveys the sense that the end-user must have a business need to disclose the exporter’s proprietary information *to third parties*. That meaning, of course, misdirects the criteria from what we think BIS intended, namely that the end-user represent (and the exporter verify) that the end-user has a genuine business need that will be served if the exporter will be permitted (by an export license) to *disclose the U.S. company’s proprietary data* to the end-user. Unless corrected, such error will confuse exporters and may cause BIS to reject applications for licenses that fail to meet the criteria that BIS intends to establish.

The criteria for an end-user to qualify as a “foreign business partner” include the additional prong or requirement that the end-user “be **contractually bound** to the U.S. company.” However, there is nothing in the words – or in the context of the definition – that delimits what kind of contractual relationship will qualify as necessary and sufficient to meet the requirement.

There is also no suggestion that the relevant contract(s) must relate to the proposed export of “cybersecurity items” that is the subject of the exporter’s license application. Experienced counsel can reasonably infer that BIS intends there to be a relationship between the required exporter/end-user contract and the proposed export of “cybersecurity items”. However, in a definition of this importance the objectives of the proposed rule would be far better served if exporters were not left to guess at the meaning of the requirement that the end-user be “contractually bound to the U.S. company” nor that their legal counsel be constrained to infer such meaning without reliable guidance from the text of the rule, other provisions in the EAR, or interpretations issued by BIS in the published rule or the relevant FAQs.

BIS appears to have foreseen the need for clarification of the phrase “contractually bound to the U.S. company” as evidenced by BIS’s insertion of an elucidating example in the parenthetical phrase that ends the definition:

“(e.g., has an **established pattern of continuing or recurring** contractual relations).”

However, in the vernacular of commercial or corporate transactions (and in the legal jargon applied to them), parties seldom, if ever, refer in contracts, agreements, or correspondence to an intention to “establish a pattern of continuing or recurring contractual relations”. Thus, there is no familiar use of that phrase or a context in which it can be set that would make it susceptible of a reliable interpretation.¹¹ Moreover, whatever is meant by a “pattern . . . of

¹¹ Moreover, the term “pattern” when it serves as an operable term in laws tends to appear in litigation contexts (e.g., “fact pattern”) and in criminal law contexts (e.g., in the definition of a RICO claim where a plaintiff or prosecutor must, among things, prove a “*pattern* of racketeering”). [Continued on next page]

contractual relations” fails to illuminate the criteria that must be met to qualify the parties as “contractually bound.”

Moreover, we think that the parenthetical introduces an unintended ambiguity: the example of “contractually bound” that it gives refers to multiple contracts (“**recurring contractual relations**”) and, in the alternative, to seemingly multi-year contracts that precede the submittal of the license application and that will extend for some indefinite period, possibly beyond the proposed export transaction (“**continuing contractual relations**”). In either event, the requirement ends with the word “relations” in the plural.

As a result, it is unclear whether BIS intends the example to be a limiting illustration – thereby requiring evidence that the exporter and end-user are “bound” or engaged in multiple contracts (whether “recurring” or “continuing”) -- or whether BIS intends instead that the parenthetical not be a limiting example and that even one contract between the exporter and end-user will suffice. The ambiguity has an additional layer: it is unclear whether “contractually bound” requires that the proposed export be the subject of or covered by such contract(s). The members of the CEECR could not reach consensus on how to interpret the parenthetical example, which seems to suggest that the example is indeed ambiguous and that it is open to quite divergent, and possibly irreconcilable, interpretations.

In order to address the potential problems discussed above, the CEECR recommends that BIS revise the term “foreign business partner” by using the following language for the note to EAR § 742.6(b)(5):

“Note to paragraph (b)(5): A ‘foreign business counter-party’¹² means a foreign based non-governmental end-user that has entered into, or proposes in writing to enter into, one or more contracts with a U.S. company and who takes appropriate actions to safeguard “cybersecurity items” to prevent the unauthorized or unlicensed reexport or transfer of such information (and include in such safeguards sufficient cybersecurity measures to prevent intrusions and exfiltration by insiders and outsiders).”

[Continued from Footnote 11 on page 31] Such usages are unhelpful aids to interpreting the meaning of the proposed rule’s phrase “an established pattern of continuing or recurring contractual relations”.

¹² We note that the term “partner” denotes a legal relationship that most commercial and corporate transactions do not create and that use of the term “partner” (which can denote “partnership” or denote “counterparty”) will not improve the export control of “cybersecurity items.” For this reason, we recommend that BIS replace the term “partner” with “counter-party”, which would suggest a contractual relationship and allow for the definition to delimit its meaning.

E. Licensing Policy for “Cybersecurity Items”

Under the proposed licensing policy set forth under the May 20 Proposed Rule, an application for export license would be “reviewed favorably” when the relevant export is destined for a U.S. company’s subsidiary located in a Country Group A:5 country such as South Korea.

The CEECR is concerned by the distinction that the proposed licensing policy attempts to draw between U.S. company subsidiaries located in a Country Group A:5 country and companies located in the same country but owned instead by nationals of that Country Group A:5 country. The distinction appears to treat license applications differently where there may not be, in fact, a significant or sufficient difference to warrant not viewing favorably the application for export to a company located in and owned by nationals of the Country Group A:5 country.

We are also concerned by the distinction that the proposed licensing policy attempts to draw between “foreign commercial partners” located in a Country Group A:5 country and a company located in and owned by nationals of the same Country Group A:5 country.

If BIS does not modify the “foreign commercial partner” category, then the policy would draw a distinction that would not necessarily serve the aims of the proposed rule. The policy would discriminate in favor of, for example, South Korean companies that manage to enter into multiple contracts with a U.S. exporter and to discriminate against South Korean companies that are seeking for the first time to be end-user recipients or seeking to enter into a commercial contract or corporate transaction for the first time with a particular U.S. exporter. Note the commercially disadvantageous consequences of a licensing policy that draws such distinction:

- A highly reliable South Korean company (with a demonstrable record of respecting and complying with U.S. export controls in multiple contracts with several different U.S. companies) is the identified end-user in a license application submitted by an exporter who has not previously transacted with the South Korean company. Such an application would not qualify to be “reviewed favorably”, even though the proposed end-user might be far more reliable an end-user (as measured by its export compliance policies, practices, and record) than a South Korean company that happens to have restricted its multiple transactions to one U.S. exporter (and thus might qualify as a “foreign commercial partner”).
- A prospective joint venture or merger or acquisition between a U.S. company and a South Korean company would involve proposed exports or transfers of “cybersecurity items” from the U.S. company to the South Korean party to the venture or corporate transaction. The parties may not have previously engaged in commercial transactions involving licensed exports. However, the South Korean company may have all of the qualifications mentioned in the preceding bullet point.

We think in both of the above-described examples the proposed licensing policy would create unnecessary obstacles to cross-border commercial and corporate transactions that the U.S. government presumably wants to encourage. Such costly hindrances could be averted by a tightly focused revision to the licensing policy.

In order to address such potential problems, the CEECR respectfully recommends that BIS adopt the following revision to the proposed licensing policy for “cybersecurity items:”

- To the categories of license applications that would be “reviewed favorably”, add a new category that would cover proposed exports of “cybersecurity items” to qualified trustworthy end-users located in Country Group A:5 countries (or a subset of such countries with whose companies it is U.S. policy to encourage transactions).
- The recommended new category would be defined as set forth in the bold text in the following excerpt of BIS’ proposed description of its licensing policy:

*“Applications for exports, reexports and transfers for cybersecurity items ... controlled for RS will be reviewed favorably if destined to ... ‘foreign commercial partners’ located in Country Group A:5, **demonstrably qualified end-users located in Country Group A:5, . . .**”*

- Add a note, immediately after the proposed *Note to paragraph (b)(5)*, which would state:

“Additional Note to paragraph (b)(5): A ‘demonstrably qualified end-user’ means a nongovernmental end-user, based in a Country Group A:5 country, that meets the following criteria: the end-user must either (i) have a record of compliance with U.S. export control laws and regulations or (ii) have provided the applicant with evidence that it has adopted and implemented cybersecurity and export compliance plans reasonably designed to avert unauthorized or unlicensed reexports or transfers (in country).”

- The note should, of course, include a comparable requirement contained at the end of the existing note to paragraph (b)(5), namely the requirement for an explanatory letter that explains:

“how the end-user meets the criteria of a ‘demonstrably qualified end-user’ located in a Country Group A:5 state and how the end-user will safeguard the items from unauthorized transfers (in-country) and reexports.”

This recommendation to add a category for license applications for exports destined to “qualified end-users in a Country Group A:5 country” would, of perforce, provide that such applications are subject to the same precautions that the proposed policy applies to applications for exports destined to “foreign business partners”: a case-by-case review to determine if the transaction “is contrary to the national security or foreign policy interests of the United States”; a “focused case-by-case review for reasons of Encryption Items (EI) control” if any “information security” functionality is incorporated in the cybersecurity item that is the subject of the license application; and, a presumptive denial if such items “have or support rootkit or zero-day exploit capabilities.”

F. Proposed EAR § 748.8(z)(1)(iii)(C)

Proposed EAR § 748.8(z)(1)(iii)(C) sets forth a requirement for an applicant's explanatory letter when the "cybersecurity items" for which an export license is applied have "not been previously classified or included in a license application . . ." ¹³ In that context, it is clearly important to the export control of intrusion technologies that BIS be informed by the applicant when the items proposed for export incorporate the highly sensitive technologies of "rootkit or zero-day exploit functionality." However, when the items for which an export license is applied merely "relate" to "intrusion software" (which itself is *not controlled* by the proposed rule ¹⁴), the license applicant should not be required to "**describe** how rootkit or zero-day exploit functionality is **precluded** from the item."

The problem with the proposed requirement rests in its asking applicants to generate descriptions of "zero-day exploit functionalities" that will often be impracticable to substantiate or will compel applicants to make exhaustive efforts to discover. Furthermore, for a license applicant to describe how rootkit or zero-day exploit functionality is *precluded* from its items or services will often prove to be beyond the applicant's ability to ascertain.

The term "**preclude**" suggests that applicants must make a potential outcome impossible or prevent it from happening. That is a task that engineers often pursue when designing safety features into a technology or system. We think, however, that in the context of "zero-day exploit functionality" in a technology or system that may contain millions of lines of software code the proposed requirement asks a company and its engineers to perform a task that will in all likelihood be extravagantly expensive to complete and thus economically beyond their reach. It will probably also be beyond their ability to ensure that their software code will not produce certain outcomes or features. It is well known that in designing software, the control of desired outcomes is usually achievable, whereas the control or avoidance of undesired outcomes is usually impossible to achieve.

We note that "zero day" vulnerabilities is a term that the proposed rule and the EAR do not define. We take the term to refer to vulnerabilities that are unknown to the designer or producer of a particular item. What makes "zero-day" vulnerabilities so sensitive is that the designer or producer of the item remains unaware of their existence, despite its best efforts to review and test the item for "zero-day" vulnerabilities.

As a result, if a potential attacker discovers such vulnerabilities, it can conduct exploits (often stealthily) against a defenseless target. Moreover, it is generally considered economically unjustifiable for a designer or producer of an item to discover all "zero-day" vulnerabilities in the item because that would entail every line of code be tested alone and in all combinations with other lines of code contained in the item. In fact, the prodigious size and complexity of contemporary software *precludes* discovery of every latent "zero-day" vulnerability in the code.

¹³ *Id.*

¹⁴ See BIS FAQs, No. 7, which states, in pertinent part: "Exploits that meet the definition of 'intrusion software' are not controlled."

“Zero-day” vulnerabilities have thus become the unknown feature in “cybersecurity items” that engineers know exists, but lamentably cannot ferret out.

Since many “zero-day” vulnerabilities are inherently undiscoverable by the designer or producer of an item, we think it impracticable and unwise to require a license applicant to “**describe** how rootkit or zero-day exploit functionality is **precluded** from the item.” It makes little sense to attempt to describe the preclusion or avoidance of vulnerabilities that the applicant has not discovered, may be financially incapable of discovering, and thus cannot develop ways of precluding.

In short, unless modified, the requirement will put applicants to the task of describing how their item precludes the very “zero-day” vulnerabilities they do not know of. We recognize that designers and producers increasingly assume that creating products without such vulnerabilities is beyond the current capabilities of virtually all designers and producers. However, knowing that as yet undiscovered “zero-day” vulnerabilities are an inherent feature of an item does not give the designer or producer the knowledge needed to “describe” how any associated “zero-day exploit functionality is precluded from the item.”

If the intent of the proposed requirement is more limited and seeks only to require that applicants describe how the design of their item prevents it from being used to exploit a “zero-day” vulnerability, the requirement as phrased does not make clear that limited scope. Moreover, even if so limited, much the same objection applies to the requirement: even items that do not contain “zero-day” vulnerabilities can be combined with other items to produce an intrusion technology and the designers of such items may not have been aware of such potential uses. Thus to require a designer or producer to describe potential uses it does not know of and to explain how it avoids them would appear to ask them to perform a futile and burdensome task.

In order to address the deficiencies discussed above, the CEECR recommends that BIS:

- Delete the requirement that an applicant “**describe** how rootkit or zero-day exploit functionality is **precluded** from the item”; and
- Replace it with the following requirement:

“(C) For items related to ‘intrusion software’ provide a certification, signed by an officer of the applicant, authorized to certify on behalf of the applicant, that after a diligent inquiry, as evidenced by end-user certifications, the applicant does not know of any rootkit or zero-day exploit functionality contained in the item and does not know of any intention by the proposed end-user to combine the item with any other items to create a rootkit or zero-day exploit functionality.”

By thus providing for an appropriately focused certification, the requirement would only necessitate that an applicant to perform a feasible and practicable set of inquiries.

XII. Conclusion

Your consideration of our comments is greatly appreciated. If you have any questions regarding this submission, please contact Geoffrey Goodale by telephone at (703) 618-6640 or by e-mail at ggoodale@tradelawadvisors.com.

Respectfully submitted,



Geoffrey M. Goodale

The Ad Hoc Coalition for Effective Export Control Reform



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0040
Tracking Number: 1jz-8kcn-p7tj

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

Purely unconstitutional. Has no benefit and only serves to mitigate interest in gun ownership.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment

This is a clear violation of the 1st Amendment and a dangerously slippery slope and I strongly oppose of it.

Due to the vague language and description it could make simply posting information of a firearm or ammunition be required to have a license and punishable without one.

Again, this "proposed rule" is unconstitutional and a violation of every citizen's freedom of speech. I am strongly opposed and will be ashamed if it is passed.

Sincerely,
Jesse

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0041

Tracking Number: 1jz-8kcn-kc06

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Jesse Anonymous



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0042

Tracking Number: 1jz-8kcn-oqqx

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

I oppose our involvement in this and specifically oppose any regulation on free speech in the discussion of firearms over the Internet. Millions of law abiding enthusiasts will be subjected to egregious regulation and criminal charges for simply posting innocently about their hobbies. The First Amendment prohibits the infringement on free press and speech. This should be scrapped.

Intel Corporation
2200 Mission College Blvd.
M/S RNB-5-125
Santa Clara, CA 95054-1537



August 3rd, 2015

ATTN: Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security
Rpd2@bis.doc.gov

Re: RIN 0694-AG32, 80 FR 31505, Revisions to Definitions in the Export Administration Regulations

Dear Ms. Hess:

Intel Corporation appreciates this opportunity to provide input to BIS in its laudable effort to harmonize terminology and regulations between the EAR and ITAR. As a major U.S. exporter and industry leader, Intel encourages further harmonization and coordination between the Departments of State and Commerce to ensure U.S. foreign policy goals are met and to advance exportability of U.S. technology and products. Intel Corporation is submitting the following public comment in response to the request issued by the U.S. Department of Commerce on proposed revisions to definitions in the Export Administration Regulations (“EAR”).

772.1 “Technology”

Intel Corporation respectfully advises BIS that the proposed revision to the definition of “technology” contradicts the EAR and ITAR where the EAR uses “Information *necessary*,” and the ITAR uses “Information *required*”. As the term “necessary” is not specifically defined in the EAR and the rest of the definition is otherwise harmonized, we suggest updating the EAR definition to read “Information required”.

Due to confusing language as written in the proposed rule, the Note to Paragraph (a)(1) should be accordingly clarified to read, “The modification of an existing item creates a new item, and technology **required** for the modification is **subject to the same controls as the new item.**”

Software source code should not be added to the EAR definition to differentiate it as “technology,” separate from object code.

734.7 “Published”

Regarding 734.7(a)(1) and (4), Intel wishes to remind BIS of the risk of intentional abuse of this allowance under the EAR, noting that simply making “technology” or “software” available to the public on the internet may not necessarily remove export controls based on commodity classification and end use.

734.8 “Technology” that Arises During, or Results from, Fundamental Research

Intel supports the clarification to the definition of fundamental research as at Intel, our Labs and other business units in research and development collaborate on publications for the wider scientific and technical community in addition to their work on proprietary research. By using this criteria, Intel will be able to implement concrete process changes to track fundamental research activities for compliance to determine if/when a research project falls under the scope of the EAR per Note 2 to paragraph (a) and becomes subject to export controls.

772.1 “Development” (General Technology Note)

Regarding the current published definition of “development”, Intel advises BIS that the term “serial production” no longer applies to the overall current technology/manufacturing environment. Considering exporters can develop, design, manufacture, and export “technology” for a single prototype or proof-of-concept which may never be serially manufactured but is still subject to the EAR, the current definition conflicts with modern business models and customer demands. For example, Intel’s Custom Foundry business unit designs, develops, and manufactures products based on customer specifications using Intel technology; these may be exported as proof-of-concept or manufactured for enterprise or consumer end-users. The development of technology required is agnostic of whether the resulting commodity will be manufactured once, or serially. Intel strongly suggests removing the word “serial” to ensure the definition of “development” focuses on refining the scope of “technology,” rather than restriction based on the type of manufacturing.

772.1 “Required” (General Technology Note)

As noted above per use of “required” vs. “necessary” in the definition of “technology,” if BIS wishes to refine technology and software to that which is peculiarly responsible for specific functionalities, the term “required” should be used consistently throughout the EAR. We believe that the extensive examples described in Note 1 and Note 2 are not necessary to include in the definition itself as they conflict with the end use controls exporters should refer to per their specific ECCN. Rather than clarifying the definition, BIS may wish to publish the example Note 1 and Note 2 as a FAQ simultaneous to the final rule to guide exporters.

734.13(b) Export and 734.14(2) Reexport

Intel Corporation strongly requests BIS to consider publishing a definition of “permanent residency” to aid exporters in establishing the appropriate country of export for foreign national license determinations. In the absence of a sufficiently broad definition to cover the variety of immigration statuses worldwide which equate to the U.S. Citizenship and Immigration Services’ *lawful permanent resident/green card holder* status, Intel recommends changing “permanent residency” to “legal residency.”

Where Intel adheres to the letter of the law on deemed exports and reexports, including following BIS’ published FAQs and guidance on third country nationals, pursuing citizenship data worldwide has become increasingly difficult due to the mobile nature of the modern workforce. “Permanent residency” as an immigration status is somewhat unique to the U.S. and other first-world nations, in contrast to other countries with sovereignty over their own immigration regulations which may not grant legal status even to foreign nationals who have permanently settled in the new country (e.g. Saudi Arabia). Particularly in cases of third country nationals and deemed reexports within multinational corporations like Intel, establishing

residency in a third country results in more confusion as various countries' immigration laws do not cleanly map to the U.S. "green card" standard. Intel requests BIS determine an EAR definition of "legal residency," such as utilizing the U.S. Citizenship and Immigration Services' lawful permanent resident status definition to establish regulatory parameters for determining equivalent international statuses, where such a legal residency status exists, e.g.:

- 1) right to reside in worksite country indefinitely
- 2) open market work authorization
- 3) admissibility without a visa
- 4) subject to deportation for crimes and without citizenship rights of voting and office holding.

Based on recent case history in industrial espionage and export violations made by U.S. persons alone, it is Intel's opinion that immigration status is not an accurate indicator of personal allegiances or risk of unauthorized export/reexport. Regulating deemed exports based on citizenship/permanent residency do not preclude willful violations of the EAR by individuals, regardless of their immigration status. If BIS wishes to control deemed exports to foreign nationals based on allegiances and personal ties to their home country, those foreign nationals who have chosen to emigrate and settle permanently in new countries with accordant long-term visa status should be afforded greater rights under the EAR with a broad, clear definition of "permanent" or "legal" residency beyond the confines of U.S. green card equivalency. By drawing a bright line between legal residency and temporary worker visa status, BIS and exporters would have fewer deemed export licenses to process, resulting in faster hiring of skilled workers and more efficient implementation of deemed export/reexport controls worldwide.

Another area of concern involves data privacy. Requiring companies to collect proof of an individual's most recent country of citizenship or permanent residency may conflict with international privacy and anti-discrimination laws. In order to avoid this conflict Intel must navigate each country's individual immigration regulation to determine if a candidate's status is equivalent and inviolably permanent in their worksite country. Creating a worldwide standard for "legal residency" which encompasses the variety of settlement statuses besides full-fledged citizenship will allow Intel to facilitate innovation and intra-company mobility of technology and employees without endlessly pursuing and tracking personal data throughout an employee's career.

734.16 Transfer (in-country)

BIS' proposal to define an in-country transfer to include "change in end use or end user" unduly extends export controls outside of the purview of exporters and requires additional compliance interdiction in the already difficult arena of end use assurances and monitoring. Exporters would be subject to an additional burden to monitor customers, partners, resellers, and third-party distributors who may not have the awareness or compliance infrastructure to ensure every transfer has appropriate export authorization. In practice, the original exporter will not be able to determine what constitutes a change in end use, or when such a change occurs. The exporter may only discover a change to end use upon request by the end user for additional services/support, by which time the retransfer has already occurred (out of the exporter's control). Due to the difficulty in tracing and tracking product downstream, exporters must rely

upon the veracity of end use statements made by customers at purchase. Following a product throughout its lifespan is infeasible; this definition is unclear as to whether the extension of transfer in-country applies to the entire range of activities, until a product is outdated or disposed of by destruction. Intel requests BIS reconsider the purpose of this definition and impact to exporters based on the limited reach of knowledge of end use beyond direct customers and lack of control over third parties' activities.

734.18 Activities that are not exports, reexports, or transfers

Requiring exporters to implement end-to-end encryption security protocols to the level of FIPS 140-2 places an undue burden and is logistically infeasible based on the size and variability of Intel's current tools and products which facilitate internal sharing. Intel recommends the FIPS compliance language be deleted from this section of the final rule, and suggests instead 734.18(a)(4)(iii) stipulate end-to-end encryption using "strong cryptographic algorithm" or other "commercially available cryptographic means"; such as 256-bit or stronger encryption. Intel could not take advantage of this highly beneficial release of "technology" shared for internal design and development.

Intel appreciates the opportunity to comment on the Proposed Rule and looks forward to continuing its cooperation with the U.S. Government on export control reform.

Best Regards,


Jeff Rittener
Senior Director, Global Trade
Intel Corporation



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0044
Tracking Number: 1jz-8kcp-33rn

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Jessie Ray

Comment

This is a direct attack on our first ammendment rights.
Freedom of speech!



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0045

Tracking Number: 1jz-8kcp-q9tx

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
D C

Comment

No, screw these changes and end this assault upon Americans, the Constitution and the Bill of Rights NOW! Repeal this crap in its entirety!



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0046
Tracking Number: 1jz-8kcq-h2eo

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Brian Patriot

Comment

I say NO to this regulation. This is a clear violation of the 1st amendment. The US government should have no authority to restrict speech, or the sharing of information that is not classified.



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security** (BIS) Proposed Rule: **Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#) 

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

ID: BIS-2015-0019-0047
Tracking Number: 1jz-8kcq-onnp

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#) 

Submitter Information

Submitter Name:
Anonymous Anonymous

Comment

1st Amendment
Free Speech
Gives us the Freedom to talk about what we want on the internet.
End of discussion.
Thank You



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: BIS-2015-0019-0048

Tracking Number: 1jz-8kcq-t17b

Comment

Document Information

After reviewing the content of proposed regulations ID#DOS-2015-0023-0001, and BIS-2015-0019-0001, I find that the proposed regulation is overbroad and needs to be updated to recognize the protections granted citizens of the United States of America under the bill of rights. In particular, the first and second amendments to the constitution of The United States of America explicitly protect the rights of the people to keep and bear arms, and to freely communicate with each other. As such, any regulation that prohibits free speech relating to the design, production, distribution, modification, use, or disposition of arms is improper and constitutes a violation of both the first and second amendment.

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Presently, many citizens of the United States of America communicate with each other openly on the internet about protected arms for all of the lawful purposes described above. Regulations which do not explicitly recognize the existing rights to arms and communication about those arms are overreaching and would have a chilling effect on free and lawful exercise of fundamental rights of citizens of the United States.

Submitter Information

Submitter Name:
Anonymous Anonymous

To comply with the constitution of The United States, any regulation put forward must not prohibit the open and public communication of information related to production of firearms, including production designs, production equipment, production software, production techniques, product distribution or marketing, techniques for modification, hardware for modification, software and software modifications embedded in firearms, techniques for use, disposal or disposition of firearms, or discussion of public policy related to any of these items.

Please review and update the afore mentioned policies to bring them into compliance with the law of the land as found

in the Bill of Rights comprising the first ten amendments to the Constitution of the United States of America.

UNIVERSITY OF MINNESOTA

Twin Cities Campus

Sponsored Projects Administration

*450 McNamara Alumni Center
200 Oak Street S.E.
Minneapolis, MN 55455-2070
612-624-5599
Fax: 612-624-4843*

August 3, 2015

Via Internet (www.regulations.gov)

Hillary Hess, Director
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, NW
Washington, DC 20230

*Re: Comments Concerning Revisions to Definitions in the Export Administration
Regulations (RIN 0694-AG32)*

Dear Ms. Hess:

The University of Minnesota's Office of Sponsored Projects Administration (the "University") respectfully submits these comments to the Bureau of Industry and Security (the "Bureau") in response to the proposed rule (the "Rule")¹ that revises several key definitions in the Export Administration Regulations ("EAR"). We applaud the U.S. Government's prodigious efforts in the ongoing Export Control Reform initiative, and are grateful for the opportunity to provide input that we hope is useful in developing an improved regime that focuses resources on transactions of real concern while reducing undue constraints on the global exchange of ideas, international commerce, and cooperation with our strategic allies.

1. Results of "fundamental research"

As a general matter, the University supports the Bureau's efforts in clarifying the fundamental research exclusion ("FRE"). In particular, the discussion of proprietary sponsor review in paragraphs 734.8(b)(1) and (2) provides welcome clarity, as do the descriptions of "basic research" and "applied research" in paragraphs 734.8(c)(1) and (2).

¹ Revisions to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31,505 (June 3, 2015).

We do, however, have concerns with two other aspects of proposed section 734.8: an overbroad element of the prepublication review language in paragraph 734.8(b), and the section’s overall ambiguous treatment of software.

A. *The “or delay” clause in the prepublication review paragraph should be removed.*

While proposed section 734.8 largely preserves the existing contours of the FRE, paragraph 734.8(b) appears to impose a broad time-based limitation that is contrary to standard academic research practice, and that might nullify the exclusion as a practical matter. The language states that data qualify for the FRE only “to the extent that the researchers are free to publish the technical data contained in the research *without any* restriction or *delay*” (emphasis added).

The “without any . . . delay” construction is unworkably vague and overbroad. Publication can be (and very often is) delayed for any number of reasons having nothing to do with the content or sensitivity of research results. Moreover, it is a standard practice and courtesy to allow research sponsors a specified period of time to review research results before publication.² Limiting the FRE to research results that will be published “without any . . . delay” could have the same practical effect as eliminating the FRE entirely—a catastrophic result for the university community, and one the U.S. Government cannot intend. The University recommends that “or delay” be deleted.

B. *The revised fundamental research exclusion should clearly encompass not only information but also software.*

There appears to be a discrepancy regarding software between the proposed texts of section 734.3 (“items subject to the EAR”) and section 734.8 (“technology” arising during or resulting from “fundamental research”). Revised paragraph 734.3(b)(3) states, in pertinent part, that the EAR do not govern “Information *and ‘software’ that . . . [a]rise* during, or result from, ‘fundamental research,’ as described in § 734.8” (emphasis added). This is materially the same as the current version of paragraph 734.3(b)(3), which describes “Publicly available technology *and software . . . that . . . [a]rise* during, or result from, fundamental research, as described in § 734.8” (emphasis added). The plural subject-verb agreement indicates that both technology/information *and* software can qualify, and will be able to qualify, for the FRE.³

Yet the proposed new version of section 734.8 seems to explain the FRE solely in terms of “technology,” which the EAR treat as being distinct from “software.” The University recommends that section 734.8 be revised to clearly encompass both “technology” *and* “software,” to be consistent with paragraph 734.3(b)(3). Moreover, given the Bureau’s position that there is no need to regulate technology/information and software differently from one another for purposes of section 734.7 (“published”), we can think of no reason to do so for purposes of section 734.8. In fact, removing

² Requirements to obtain substantive sponsor *approval* to publish results, as opposed to mere review, are not typical. We agree such conditions are generally inconsistent with the FRE.

³ This interpretation is confirmed by the long-standing exclusion of certain 5D002 encryption software from the FRE, as stated in the existing text of paragraph 734.8(a). If all software in general were outside the scope of the FRE, such language about encryption software in particular would be redundant and nonsensical.

software from the scope of the FRE would be a substantive and disastrous change—well beyond a mere clarification—in the requirements governing the academic research community.

2. The vague qualifiers “general” and “commonly” should be considered for removal from paragraph 734.3(b)(3)(iii).

Paragraph 734.3(b)(3)(iii) excludes from the EAR information and software that concern “general scientific, mathematical, or engineering principals” that are “commonly taught in schools” and released in academic fora. The University recommends that BIS consider removing “general” and “commonly” from this clause. These words strike us as inherently subjective. At what point does a course about satellites and orbital mechanics cross the line from “general” to specific? What percentage of universities must offer laboratory seminars about high-performance nanocomposites for the content to become “commonly” taught? “General” and “commonly” are vague, problematic concepts for compliance programs and, we can imagine, in enforcement situations.

3. Conclusion

Please don’t hesitate to contact me at bris0022@umn.edu or 612-625-3860 with any questions regarding these comments. Thank you for your efforts, and for encouraging public participation in the conversation on Export Control Reform.

Respectfully submitted,

/s/

J. Patrick Briscoe

Export Controls and International Projects Officer



Comment on FR Doc # 2015-12843

This is a Comment on the **Bureau of Industry and Security (BIS) Proposed Rule: Definitions in the Export Administration Regulations**

For related information, [Open Docket Folder](#)

Comment Period Closed
Aug 3 2015, at 11:59 PM ET

Comment

Dear Lawmakers,

I believe this is a blatant attempt to circumvent my Constitutional rights under the First and Second Amendments. Online forums are a public place as many do not require membership.

This will harm gunsmiths, manufacturers, reloaders, and do-it-yourselfers who all require the ability to obtain and/or distribute the information they rely on to conduct their businesses.

The First and Second Amendments must not be subverted to enable "legal" governmental misuse of the Fourth Amendment.

I urge you to repeal these new regulations in their entirety. The First and Second Amendments are still the law of the land!

Sincerely,

Christopher Wyngarden

ID: BIS-2015-0019-0050

Tracking Number: 1jz-8kcr-w3bg

Document Information

Date Posted:
Aug 4, 2015

RIN:
0694-AG32

[Show More Details](#)

Submitter Information

Submitter Name:
Christopher Wyngarden

RE: RIN 0694–AG32

July 29, 2015

PUBLIC COMMENT

This is a public comment to RIN 0694–AG32, as published by the Department of Commerce Bureau of Industry and Security (“BIS”) at 80 Fed. Reg. 31,505 (June 3, 2015) (the “Proposed Rule”), titled, “Revisions to Definitions in the Export Administration Regulations.”

I. COMMENT ON STATUS OF EXPORT CONTROL REFORM

The Proposed Rule is published as part of the President’s Export Control Reform (“ECR”) Initiative, which it claims “will enhance U.S. national and economic security, facilitate compliance with export controls, update the controls, and reduce unnecessary regulatory burdens on U.S. exporters.”

ECR promised a single export control list, single export control agency, and single information technology (“IT”) system. Industry reasonably expected that these changes would update, simplify, and increase efficiency of the system. This would in turn make the system more robust, industry friendly, and better support national security objectives.

Unfortunately, following over half a decade of complex regulatory amendments, ECR has not established a single export control list, single export control agency, or a single IT system. Instead, the reform has vastly increased the complexity of already overly complex regulations. This has significantly increased the compliance burden and costs on industry without the benefits of a single list, single agency, or single IT system.

Concerns with ECR changes in the Proposed Rule are discussed below. Suggested revisions are provided where appropriate.

II. REMOVAL OF SUPPLEMENT NO. 1 TO PART 734

Export compliance professionals and other members of the public look to Supplement No. 1 to Part 734, “Questions and Answers—Technology and Software Subject to the EAR” (“Supplement No. 1”) to determine how to use exclusions for the release of technology at open conferences, publications, educational instruction, and fundamental research under the Export Administration Regulations (“EAR”). It is perhaps the clearest and most useful part of the regulations.

Nevertheless, at page 31,507 of the Proposed Rule, the ECR Task Force proposes to remove Supplement No. 1 and bury it among an increasing archive of web site guidance. The stated agency rationale for this removal is that “[q]uestions and answers are illustrative rather than regulatory and are thus more appropriately posted as Web site guidance than published as regulatory text.”

Supplement No. 1 is regulatory - i.e., it is a codified regulation that carries the force of law. The fact that it is also illustrative does not justify its removal from the EAR. To the contrary, industry experience over the years has shown that the illustrations provided by Supplement No. 1 are essential when determining how to apply EAR exclusions to real world situations.

In contrast to the present regulatory status of Supplement No. 1, agency web site guidance is not law and can be changed at any time. Moving Supplement No. 1 to a web site page therefore presents a problem because changes to the substantive scope of the EAR should be made through proposed regulatory amendments subject to public notice and comment. These safeguards are lost if Supplement No. 1 is moved to a web page, outside of the regulations, where agency officials can change it without notice. Accordingly, Supplement No. 1 must not be removed unless all its substantive provisions are adequately incorporated into Part 734 or elsewhere in the regulations.

III. PROPOSED DEFINITION FOR “APPLIED RESEARCH”

“‘Fundamental research’ means **basic and applied research** in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.” National Security Decision Directive 189 (emphasis added).

The definition for “basic research,” as listed in Section 734.8 of the Proposed Rule, is the same as that already defined in the EAR Section 772.1, which matches the definition for “basic scientific research” in the Wassenaar Arrangement’s General Technology Note.

There is no existing EAR definition for “applied research” in the EAR or the Wassenaar, so the Proposed Rule seeks to add Section 734.8(c)(2) to define “applied research” to mean “the effort that:”

- Normally follows basic research, but may not be severable from the related basic research;
- Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and
- Attempts to advance the state of the art.

This proposed definition does not define what is generally understood to constitute applied research. In applied research, the objective is to gain knowledge or understanding necessary to determine how a recognized need may be met. Such intent is the essence of applied research and what distinguishes it from basic research. However the proposed definition for “applied research” at Section 734.8(c)(2) fails to state that applied research must be for a specific need, end use, application, etc. At best, it is vague in this respect and, as a result, overlaps with definition for basic research. Of course, some research may consist of both basic and applied elements, but the demarcation between the definitions should be maintained.

In addition, the proposed definition is different from the definition set forth in the 2014 Office of Management and Budget Circular A-11, which defines applied research as:

Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.

The OMB definition is used in state and local grants, federal programs (e.g., DoD Budget Category 6.2 Funding), and is used by the National Science Foundation. Accordingly, EAR use of the term should follow the OMB definition.

IV. ACTIVITIES THAT ARE NOT DEEMED REEXPORTS

The Proposed Rule seeks to codify the Deemed Reexport Guidance posted on the BIS web site, the stated intent of which is to create provisions in the EAR for EAR technology and source code similar to the license exemptions contained at sections 124.16 and 126.18 of the International Traffic in Arms Regulations (“ITAR”).

Under the proposed Section 734.20, the release of technology or source code by an entity outside the United States to a foreign national of a country other than the foreign country where the release takes place does not constitute a deemed reexport if a variety of conditions are met, to include:

- The entity is authorized to receive the technology or source code at issue, whether by a license, license exception, or through situations where no license is required under the EAR;
- The foreign national is a *bona fide* regular and permanent employee (who is not a proscribed person under U.S. law) directly employed by the entity;
- Such employee is a national exclusively of a country in Country Group A:5; and

- The release of technology or source code takes place entirely within the physical territory of any such country.

This proposal also seeks to add a definition for “proscribed person” at Section 772.1.

This new decontrol is proposed as an exclusion from EAR control and not as an exception to EAR license requirements. This approach is inconsistent with BIS’ stated intent, which is for the EAR to mirror certain ITAR license exemptions. This approach is also likely to create substantial confusion because the requirements of Section 734.20 are more characteristic of a license exception than an exclusion from EAR control.

Exclusions from export controls generally cover straightforward situations that are entirely excluded from regulatory requirements. In contrast to these, the type of decontrol proposed under Section 734.20 requires the presence of several conditions and technology and source code exported under it will apparently remain subject to EAR control. Accordingly, instead of mirroring the relevant ITAR exemptions through a new exclusion at Section 734.20, BIS should consider implementing a new EAR exception at Part 740.

V. DEFINITION FOR “PECULIARLY RESPONSIBLE”

The Proposed Rule seeks to define “peculiarly responsible” based on the catch-and-release structure used for the definition of “specially designed.” However, similar to the definition of specially designed, the proposed definition for peculiarly responsible is much too long and complicated.

Industry is still grappling with the definition for specially designed. Instead of duplicating this confusion with another convoluted definition that only a few people understand, BIS should use the generally understood meanings of “peculiar” and “responsible” to form a definition of peculiarly responsible.

For example, Merriam-Webster defines “peculiar” as “characteristic of only one person, group, or thing”; and defines “responsible” as “having the job or duty of dealing with or taking care of something or someone.” Considering these definitions, perhaps “peculiarly responsible” can simply mean “an item having a distinctive characteristic that performs a job essential to achieving or exceeding controlled performance levels, characteristics or functions at issue.”

VI. PROPOSED EXCLUSION FOR ENCRYPTED TECHNOLOGY

Page 31,509 of the Proposed Rule explains that BIS seeks to add Section 734.18(a)(4) to establish a specific carve-out from the definition of “export” for the transfer of technology and software that is sufficiently protected with end-to-end encryption.

The Proposed Rule further notes, “transfer in encrypted form consistent with the requirements of paragraph (a)(4) poses no threat to national security or other reasons for control and does not constitute an “actual” transmission of “technology” or “software.””

The proposed text of the new exclusion is as follows:

§ 734.18 Activities that are not exports, reexports, or transfers.

(a) The following activities are not exports, reexports, or transfers:

* * *

(4) Sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and

(iv) Not stored in a country listed in Country Group D:5 (*see* Supplement No. 1 to part 740 of the EAR) or in the Russian Federation.

Email containing otherwise controlled technology may, without the knowledge of the sender, transit a foreign country’s Internet service infrastructure en route to its intended and authorized final destination. Relevant here, the Proposed Rule prohibits storage in a country listed in Country Group D:5 or in the Russian Federation, but it does not define what BIS will consider “storage” on a foreign server or other drive.

Absent some limits on application of the term “storage,” the term can reasonably be construed to mean even temporary storage incidental to email routing through foreign servers. Because of this, as literally applied, proposed subsection 734.18(a)(4)(iv) can prohibit encrypted unclassified technical data transmitted by emails if such emails transit servers in a Country Group D:5 country or the Russian Federation. Because email transit routes are generally unknown, companies using the proposed exemption for communications of encrypted technology will face unknown risks of inadvertent violations involving Country Group D:5 countries and the Russian Federation.

* * *

Thank you for your consideration.

Yours truly,

ON BEHALF OF THE FIRM



Matthew A. Goldstein, Principal Counsel
MATTHEW A. GOLDSTEIN, PLLC
1012 14th Street NW, Suite 620
Washington, D.C. 20005
Tele: (202) 550-0040
Email: matthew@goldsteinpllc.com



*Export Regulation Office
600 14th ST NW Suite 300
Washington, DC 20005*

VIA E-MAIL (publiccomments@bis.doc.gov AND DDTCPublicComments@state.gov)

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

Mr. C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
Washington, DC 20522

August 3, 2015

REF: RIN 0694-AG32 (BIS) AND RIN 1400-AD70 (DDTC)

RE: Comments on Proposed Revisions to Certain EAR and ITAR Definitions

Dear Ms. Hess and Mr. Peartree:

On behalf of International Business Machines Corporation (“IBM”), we are submitting these comments in response to the June 3, 2015 notices published by the Departments of Commerce and State concerning proposed revisions to definitions in the Export Administration Regulations (“EAR”) and International Traffic in Arms Regulations (“ITAR”) as stated in the above reference (“Proposed Rules”). These comments are timely submitted by the due date noted in the Proposed Rules.

IBM provides information technology products and services to customers in over 175 countries, and employs more than 379,000 persons across 75 countries worldwide. 2014 revenues were \$92 billion, of which over 60 percent was generated outside the United States. As IBM’s operations are both vast and diverse, a robust internal control program is required to ensure compliance with export regulations. Changes to the definitions within the regulations will affect the execution of the program as various areas would be impacted by the Proposed Rules, including, but not limited to the following:

- IBM’s engagements involving items subject to the ITAR;
- IBM’s use of cloud services for both internal and external purposes;

- Employment of foreign persons; and
- IBM's research and development functions responsible for determining the export classification of source code and technology.

IBM thanks both Departments for the opportunity to provide comments on the potential impact of the Proposed Rules. IBM supports the efforts undertaken by the Departments to improve and, wherever possible, harmonize the definitions used within the regulations as part of the Obama Administration's ongoing Export Control Reform ("ECR") initiative. It is IBM's position that many of the proposed definitions that are set forth in the Proposed Rules are an improvement on the current EAR and ITAR regulations. In particular, IBM greatly appreciates the proposed amendments to the ITAR definitions of "defense article," which would now include software and "defense services," thereby clarifying that servicing an item subject to the EAR which has been installed into a defense item would not be considered an ITAR-controlled activity.

IBM would like to offer the following recommendations for further improvements to the Proposed Rules.

RECOMMENDATIONS

1. Activities That Are Not "Exports," "Reexports," or "Transfers" (EAR § 734.18) (ITAR § 120.52)

The Proposed Rules create an exclusion from the definitions of "export," "reexport," and "transfer" for unclassified technology or software secured with end-to-end encryption using specific cryptographic modules following NIST standards and not stored in specific countries. The EAR Proposed Rule includes a provision which allows flexibility in the cryptographic methods used to meet the exclusion by including the statement "other similarly cryptographic means," whereas the ITAR Proposed Rule is rigid in its implementation.

IBM is appreciative of the exclusion and believes it will benefit industry by simplifying compliance with respect to cloud storage solutions and email transmissions; however, the use of cloud is much more pervasive and includes cloud-based software-as-a-service (SaaS) solutions and platform-as-a-service (PaaS) solutions, among others. As a result, additional exclusions are necessary to allow more freedom of action in this rapidly growing space. There is also a concern with the ITAR's proposed language, as it does not allow for industry to determine the best methods for protecting data. In addition, the referenced NIST guidance and certification requirements were not easily found.

RECOMMENDATION: IBM recommends that the proposed exclusion language in the EAR be adopted for both regulations. In addition, information on the referenced NIST guidance and certification requirements needs to be readily accessible on the Departments' web sites so users are more easily able to find the information. Lastly, IBM recommends that additional exclusions or exceptions be adopted in both regulations that would benefit cloud service providers and users

beyond the end-to-end encryption solutions for storage and email transmissions. Specifically, it would be helpful if two additional provisions were included:

- a. Exclusion for the intracompany use of cloud solutions by foreign nationals directly employed by entities which have implemented a robust compliance program; and
- b. Exclusion in the end-to-end encryption requirement for the decryption of data by the cloud user to perform operations within the cloud environment.

2. Activities That Are Not “Exports,” “Reexports,” or “Transfers” (ITAR § 120.52)

The ITAR Proposed Rule includes a provision which allows authorized foreign persons to hand carry technology and software subject to the ITAR; however, each use of this provision by the authorized foreign person must be documented.

In order for a foreign person to be authorized to obtain the technology and software in the first place, the exporter would have had to complete the export licensing process and been granted an approval. The approvals contain various provisos for use of the authorization, with which the exporter would be responsible for ensuring compliance. Adding a proviso independent from the licensing process may cause confusion for the exporter as both the license and the regulations would have to be consulted.

RECOMMENDATION: IBM recommends that any documentation requirements should be included within the licensing provisos.

3. Activities That Are Not “Deemed Reexports”

A. Requirement to Be “Certain” (EAR § 734.20(a)(2))

In the BIS Proposed Rule, a “deemed reexport” does not occur if the “technology” or “source code” is released to a foreign national, provided the entity has received it under an export authorization (i.e., license, license exception, or NLR) and, per subparagraph (a)(2), the entity must be “certain” about the foreign national’s most recent citizenship.

The term “certain” indicates that the exporter must have the information verified to a level without any doubt. IBM is concerned with the amount of documentation required to achieve this standard, as well as the level of investigation needed to remove any uncertainty. Under normal hiring practices, identity and employment verification relies on standard documentation requirements (i.e., passport, permanent resident cards, and visas). This is the standard which export regulations should follow so no additional administrative burden is placed on the exporter.

RECOMMENDATION: IBM recommends the removal of the “certain” standard from the proposed language and instead to the use of a knowledge standard that is based on documentation obtained during normal hiring practices.

B. Requirement to Screen for “Substantive” Contacts (EAR § 734.20(c))

Under the proposed section, subparagraph (c) allows for an exclusion to nationals outside of Country Group A:5 as long as various conditions have been met. Under (c)(5)(ii)(B) – (D), the requirements include the need to screen the employee for “substantive” contacts with countries listed in Country Group D:5, with records maintenance at a minimum of 5 years or the duration of the employment.

This requirement is problematic in that “substantive” is an undefined term and is therefore, open to interpretation by both the exporter and the regulator. Secondly, normal business practices do not invoke a continuous screening of an individual once they have become an employee. As a result, this requirement would add administrative burden as well as a cost for conducting the additional screening throughout the span of the employee’s tenure at the company. Thirdly, there is no carve out for contact with D:5 countries on behalf of the employer who may lawfully conduct business operations within the specified countries.

RECOMMENDATION: IBM recommends removal of the ongoing screening requirements from the exclusion. If this is not possible, IBM instead recommends the introduction of an exclusion for contact with D:5 countries as part of the individual’s defined work scope.

4. “Peculiarly Responsible” (EAR § 772.1) (ITAR § 120.46)

The proposed definition of “peculiarly responsible” is a welcome addition to the regulations; however, it now modifies the terms which are currently included under the existing “required” definition, resulting in the introduction of the “catch and release” construct similar to that which was implemented for the term “specially designed.” “Peculiarly responsible,” though not defined, is a well understood concept by industry and easily explained to technical engineers and developers. The “catch and release” mechanism introduces additional complexity in that those technical personnel will now require a much broader understanding of the regulations to determine what may be controlled only for specific reasons, what may be classified as EAR99 or classified under a commodity jurisdiction, what the intent for which the item was developed, and if the item is identical to information used with items already in production. This additional complexity will complicate the classification exercise, require the inclusion of additional persons to perform this exercise, and increase the risk of classification errors by well-intentioned technical personnel who are not expert in the export regulations.

RECOMMENDATION: IBM recommends removal of the “catch and release” construct in the definition and limit the definition to “the technology or source code responsible for allowing an enumerated item to exceed the controlled performance levels, characteristics or functions.”

5. “Release” (EAR §734.15; ITAR §120.50)

The proposed definition of “release” in the Proposed Rules under subparagraph (a)(1) includes “visual or other inspection” by a foreign person which reveals a controlled defense item or

“technology” or “source code” subject to the EAR. The newly defined term fails to indicate what level of access is subject to the control, which has been a historical area of confusion for industry. Specifically, does the “release” include both theoretical access and actual access, or is it limited to when an identifiable release has occurred? As an example, if a foreign person is given general access to a server which contains a database of controlled technical data, theoretical access has occurred; however, it is not until that individual visually inspects the contents of the database that controlled technical data has been provided.

RECOMMENDATION: IBM recommends both definitions be revised to indicate that “release” only occurs when EAR or ITAR controlled “technology” or “source code” has been visually inspected.

6. “Transfer” (In-Country) (EAR § 734.16) and “Retransfer” (ITAR § 120.51)

The proposed EAR definition of “transfer” and the proposed ITAR definition of “retransfer” include a change in end use as part of the defined term. This is an expansion on the current reach of the regulations. To determine a change in end use would require an exporter to continuously monitor how the exported item is being used by the third party. In a traditional sales environment, an exporter would not have visibility to how an exported item is being used unless the exporter and recipient were in a joint agreement which extends the relationship past the point of sale. This is not a typical sales model, and this level of knowledge would not be attainable during the normal course of business. Once a traditional sale is complete, the information on how the product is being used is not available.

RECOMMENDATION: IBM recommends the definitions be revised to remove a change in end use. Alternatively, the definition should be modified to indicate the obligation for the “transfer” or “retransfer” is on the ultimate consignee, not the original exporter.

7. “Defense Services” (ITAR § 120.9)

Under the proposed definition of “defense service,” the Note to paragraph (a) lists various activities which are not included as a “defense service.” The exclusions, specifically under number 3, include the servicing of items subject to the EAR, except as described in paragraph (a)(5) of this section. However, under (a)(5), the furnishing of assistance on a defense article or an item specially designed for a defense article to the government of a §126.1 listed country is a controlled defense service. As (a)(5) clearly defines that the items must be a defense article or an item specially designed for a defense item, the items would not be “subject to the EAR.” This automatically disqualifies the activity described in exclusion number 3 to the Note to paragraph (a). As a result, the reference to the exclusion in (a)(5) is not required.

RECOMMENDATION: IBM recommends the removal of the reference to the (a)(5) exclusion in number 3 to the Note to paragraph (a).

8. “Public Domain” (ITAR § 120.11)

Under the ITAR Proposed Rule, eligibility for the release into the “public domain” of “technical data” or software hinges on a requirement to obtain a pre-approval through one of several listed U.S. government sources. In addition, in Note 1, a user is ineligible to further export, reexport or transfer information in the “public domain,” if that user has “knowledge” that the information was placed in the “public domain” without obtaining the required authorizations.

The ability to place “technical data” or software in the “public domain” is protected under the First Amendment of the Constitution (i.e., freedom of speech). Placing pre-publication requirements would be a violation of an individual’s fundamental rights.

Further, depending upon the interpretation of Note 1, this Note potentially places an unnecessary burden and a risk of violation on persons which would like to further export, reexport or transfer information from a published source. The Department arguably could take the view that due diligence in this context includes verification of an existing authorization. Such an interpretation would place a burden on the user for information which has been placed in a medium where the data is considered to be freely available without restriction. In addition, without performing due diligence, any future dissemination of the data puts the user at risk of violating the regulations.

RECOMMENDATION: IBM recommends that the pre-publication requirement on information being released into the “public domain” as well as Note 1 be removed from the final rule. If Note 1 is maintained, IBM recommends that the Department specify that there is no affirmative duty on the part of users to inquire about the authorization status of information found in the “public domain.”

* * *

In addition to the specific recommendations previously described, IBM believes that definitions should be consistently listed in the definitions sections of each regulation (i.e. EAR § 772 and ITAR § 120). Interspersing some definitions within the regulatory text and others within the definition sections causes confusion for industry and increases the risk of error. Placement consistency will help to alleviate that issue.

IBM feels these are the most critical changes necessary to ensure the Proposed Rules are able to be easily implemented and understood. We thank you for the opportunity to comment.



Lillian M. Norwood
Manager, Export Regulation Office
Government & Regulatory Affairs
IBM Corporation



OFFICE OF THE VICE PRESIDENT FOR
RESEARCH AND ECONOMIC DEVELOPMENT

2660 University Capitol Centre
Iowa City, Iowa 52242-5500
319-335-2119

August 3, 2015

Director Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW
Washington, DC 20230

Via email to: publiccomments@bis.doc.gov

RE: RIN 0694-AG32: Comments to proposed revisions in the Export Administration Regulations

Dear Director Hess:

The University of Iowa ("Iowa" or "University") is one of the nation's top public educational and research universities, with over \$438M in external funding during the last fiscal year. Iowa is a member of the Council on Government Relations ("COGR") and the Association of American Universities ("AAU"), which represents many of the country's elite public and private research-intensive universities.

Iowa appreciates this opportunity to provide its perspective to the Department of Commerce regarding the proposed revisions to various definitions in the Export Administration Regulations ("EAR") to enhance clarity and consistency with the International Traffic in Arms Regulations ("ITAR") and update and clarify the application of controls to electronically transmitted and stored technology and software. The University supports the comments submitted by COGR and AAU, but wishes to specifically comment on the impact particular proposed changes would have on its educational and research missions.

§734.3(b)(3)(iii) "Education Exemption". The proposed restatement of the "education exemption" in EAR §734.3(b)(3)(iii) incorporates some current language of ITAR §120.10(b) to state "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, **and** released by instruction in a catalog course or associated teaching laboratory of an academic institution." The University suggests the "**and**" be changed to "**or**" to clearly include catalog courses in areas of emerging technology as well as associated teaching laboratories.

§734.8(a) as it relates to “fundamental research,” “technology,” and “software.” Currently §734.3(b)(3) of the EAR states in part that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. Proposed §734.3(b)(3) and §734.7(a) treat technology and software similarly. However, under proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is “intended to be published" would not be subject to the EAR. To address this apparent inconsistency and considering how research findings resulting from fundamental research may be written in natural language or computer language, Iowa suggests the proposed rule clarify that software arising during, or resulting from, fundamental research is not subject to the EAR.

§734.8(c) Fundamental Research Definition. To decrease anticipated disputes about whether research extends beyond “applied research” and then erodes the fundamental research definition, The University suggests omitting definitions of basic and applied research in §734.8(c) and retaining a stated presumption, as is currently in §734.8(b), that university research is fundamental.

§734.13(a)(6) Export defined to include release or transfer of decryption keys. Iowa supports how proposed §734.13(a)(6) introduces a knowledge element for determining when an “export” occurs.

§734.18(a)(4)(iii) and (iv) Sending, taking or storing technology or software. The University supports the option in §734.18(4)(iii) of providing for “other similarly effective cryptographic means” for securing technology or software. With respect to the restriction in §734.18(a)(4)(iv) on countries not listed in Country Group D:5 or the Russian Federation, Iowa suggests BIS further consider the impact of most cloud providers insisting on storing data internationally. To address that reality, BIS may want to add a note to clarify that sufficient individual compliance can be accomplished and documented by imposing a contractual obligation on a provider/vendor.

Iowa commends the Department of Commerce for undertaking this effort and appreciates the opportunity to provide its perspective on these issues.

Sincerely,



Daniel A. Reed
Vice President for Research and Economic Development
Computational Science and Bioinformatics Chair
Professor of Computer Science, Electrical and Computer Engineering, and Medicine

Robert L. Clark
Senior Vice President for Research



By email to publiccomments@bis.doc.gov, subject "RIN 0694-AG32"

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC

Subject: RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*

Dear Ms. Hess:

The University of Rochester appreciates the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*.

We support the efforts of the Departments of Commerce, Defense, and State to rationalize, clarify, and focus U.S. export controls. RIN 0694-AG32 and the accompanying RIN 1400-AD70 regarding revisions to ITAR definitions, include elements of progress toward harmonized and constructive definitions of terms.

We believe the harmonized definitions are an important step forward. On the whole they represent substantial progress in achieving meaningful export control reform, with many helpful changes and clarifications (e.g. redefinition of "release," clarification that submission of manuscripts to journal editors constitutes "published" information). As such, the University of Rochester supports the joint comment letter submitted by the Association of American University, Council of Governmental Relations and Association of Public and Land-grant Universities

The University of Rochester would like to specifically emphasize the following points raised in the AAU/COGR/APLU joint comment letter in response to select issues on which BIS has requested specific comments.

- *Whether the proposed revisions create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR:* There is a major disconnect between the proposed EAR and ITAR definitions in their treatment of prepublication review to assure that publication does not divulge a sponsor's proprietary information. EAR 734.8 continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published." ITAR 120.49 states that technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data without any restriction or delay, including research sponsor proprietary information review. **We strongly oppose this proposed change to the ITAR that would now exclude any research subject to prepublication review from being considered fundamental research. We urge that the ITAR be aligned with the EAR.**

- *Whether the alternative definition of fundamental research suggested in the preamble should be adopted:* Currently the EAR (§734.3(b)(3)) states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. The proposed 734.3(b) (3) and 734.7(a) also treat technology and software similarly. However, under the proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is "intended to be published" would not be subject to the EAR. This change would significantly complicate and restrict university research. Research findings resulting from fundamental research may be written in natural-language or computer language. In either case it is "technology" that should be able to be freely shared as arising during or resulting from fundamental research. No explanation is provided as to the reason for changing the recognition of the similarities between software and technology in the current EAR (734.2(b); 734.7(b)). We strongly recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.
- *With respect to end-to-end encryption as described in the proposed rule (sec. 734.18), whether the illustrative standard in the proposed EAR rule also should be adopted in the ITAR; whether the safe harbor standard in the proposed ITAR rule also should be adopted in the EAR, or whether the two bodies of regulations should have different standards:* We appreciate that the proposed rules address cloud computing situations, which have been an area of considerable uncertainty under the current rules. BIS asks for comments as to which proposed rule more clearly describes the intended control. We prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national.
- *The effective date of the final rule:* BIS proposes a 30-day delayed effective date. Changes to ECCNs generally have had a six-month delayed effective date while other rules affecting export controls have been effective on the date of publication. We support a six-month delayed effective date.

In closing, we again want to express our appreciation to BIS for their responsiveness to many of the issues and concerns that universities have raised. We believe the EAR changes are mostly positive and deserving of support. We hope BIS will consider the comments of AAU/COGR/APLU in finalizing the proposed definitions, and appreciate the opportunity to comment.

Sincerely,



Robert L. Clark
Senior Vice President for Research

AAU *Association of American Universities*
APLU *Association of Public and Land-grant Universities*
COGR *Council on Governmental Relations*

August 3, 2015

Kevin Wolf
Assistant Secretary of Commerce for Export Administration
Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230

Via Email: publiccomments@bis.doc.gov

Re: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32)

Dear Assistant Secretary Wolf:

Enclosed please find comments from the Association of American Universities, the Association of Public and Land-grant Universities, and the Council on Governmental Relations on the Department of Commerce Bureau of Industry and Security Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32). Our staff is available to provide more information or discuss these matters further should you have any questions regarding our comments.

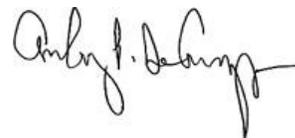
Sincerely,



Hunter R. Rawlings III
President
AAU



Peter McPherson
President
APLU



Anthony DeCrappeo
President
COGR

Attachment 1

AAU Association of American Universities
APLU Association of Public and Land-grant Universities
COGR Council on Governmental Relations

MEMORANDUM

August 3, 2015

TO: Regulatory Policy Division, Bureau of Industry and Security, U.S. Department of Commerce

FROM: Association of American Universities

Contact: Tobin Smith, toby.smith@aau.edu (202) 408-7500

Association of Public and Land-grant Universities

Contact: Jennifer Poulakidas, jpoulakidas@aplu.org (202) 478-5344

Council on Governmental Relations

Contact: Robert Hardy, rhardy@cogr.edu (202) 289-6655

Re: RIN 0694-AG32

Revisions to Definitions in the Export Administration Regulations

On behalf of the over 200 universities represented by our associations, we greatly appreciate the opportunity to comment on the revision of definitions relating to the export administration regulations (RIN 0694-AG32).

The Association of American Universities (AAU) is an association of 60 U.S. and two Canadian leading research universities organized to develop and implement effective national and institutional policies supporting research and scholarship, graduate and undergraduate education, and public service in research universities. The Association of Public and Land-grant Universities (APLU) is a research, policy, and advocacy organization of 238 public research universities, land-grant institutions, state university systems, and affiliated organizations, dedicated to increasing degree completion and academic success, advancing scientific research, and expanding engagement. The Council on Governmental Relations (COGR) is an association of 190 U.S. research universities and their affiliated academic medical centers and research institutes that concerns itself with the impact of federal regulations, policies, and practices on the performance of research and other sponsored activities conducted at its member institutions.

Our associations value the close working relationship that we have established over the years with BIS and appreciate the opportunity to comment on harmonized export control related definitions. We believe the harmonized definitions are an important step forward. On the whole they represent substantial progress in achieving meaningful export control reform, with many helpful changes and clarifications (e.g. redefinition of "release," clarification that submission of manuscripts to journal editors constitutes "published" information). Below are our associations' joint comments in response to the eight issues on which BIS has requested specific comments:

1. Whether the proposed revisions create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR.

Response: There are a number of inconsistencies between the EAR and ITAR which are either relatively minor

or reflect longstanding practices. However, there is a major disconnect between the proposed EAR and ITAR definitions in their treatment of prepublication review to assure that publication does not divulge a sponsor's proprietary information. EAR 734.8 continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published." ITAR 120.49 states that technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data without any restriction or delay, including research sponsor proprietary information review.

The proposed ITAR interpretation of sponsor proprietary information review greatly concerns our associations, since it is currently common practice for company sponsors to require proprietary information review for university contracted and subcontracted research. The effect of the proposed ITAR provision is to remove any research projects involving defense articles subject to such review from fundamental research. This will have a chilling effect on innovation and university-industry partnerships. No explanation is provided as to the reason for the different policies. We strongly oppose this proposed change to the ITAR that would now exclude any research subject to prepublication review from being considered fundamental research. We urge that the ITAR be aligned with the EAR interpretation and definition of fundamental research.

Other points of difference are the provisions related to government-sponsored research covered by contract controls (EAR 734.11). The proposed EAR rule essentially restates the current 734.11(a), which universities have found confusing. We prefer the ITAR language at 120.49(b) Note 3, suitably modified to apply to technology arising during or resulting from fundamental research. The examples in 734.11(b) are helpful and should be retained.

A change in the proposed EAR rule of particular relevance to educational institutions is the proposed restatement of the "education exemption" in the current EAR 734.9, which is removed. The new statement in the proposed EAR 734.3(b)(3)(iii) merges current ITAR (120.10(b)) and EAR text to state "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." We suggest that the "and" be changed to "**or**" to avoid unintentionally limiting this section, i.e. to clearly cover a new university course in an emerging technology area so long as it is included in a course catalog.

2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted.

Response: The proposed alternative definition would read: "Fundamental research means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." This appears to restate the current definition in a shorter fashion, and on its face we do not see a sharp distinction. However, there may be some vagueness in the term "non-proprietary." In fact, the proposed ITAR rule discussed above demonstrates confusion about what constitutes non-proprietary research. Additionally we urge significant caution in changing a definition of fundamental research that has been endorsed by White House Administrations of both parties over the years and that has served the scientific community well.

Currently the EAR (§734.3(b)(3)) states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. The proposed 734.3(b)(3) and 734.7(a) also treat technology and software similarly. However, under the proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is "intended to be published" would not be subject to the EAR. The

proposed rule preamble refers to a proposed note "to clarify that software and commodities are not 'technology resulting from fundamental research'" (although we were unable to locate the note in the Federal Register notice).

In addition to the internal inconsistency, this change would significantly complicate and restrict university research. Research findings resulting from fundamental research may be written in natural-language or computer language. In either case it is "technology" that should be able to be freely shared as arising during or resulting from fundamental research. No explanation is provided as to the reason for changing the recognition of the similarities between software and technology in the current EAR (734.2(b); 734.7(b)). We strongly recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.

We also note with concern that the current presumption in EAR 734.8(b) that university based research will be considered fundamental research appears to have been eliminated. There is no clear policy reason stated for this change. The applicability should continue to be determined by the other criteria in 734.8(b). We urge BIS to restate the presumption in the final rule.

Finally, the proposed EAR 734.8 Note 1 to paragraph (a) states: "The inputs used to conduct fundamental research, such as information, equipment, or software, are not "technology that arises during or results from fundamental research" except to the extent that such inputs are technology that arose during or resulted from earlier fundamental research." We believe the statement may be misleading. Official government policy on the transfer of scientific and technical information as reflected in National Security Decision Directive (NSDD) 189 states that "No restrictions may be placed upon the **conduct** [emphasis added] or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes." Conduct of fundamental research may draw upon a wide range of information and other inputs. In drawing a sharp distinction between the conduct and results of fundamental research, BIS appears to be arbitrarily restricting NSDD-189 without clear authority. We question the need for this statement and urge that it be removed.

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

Response: The EAR changes include definitions of "basic research" (734.8, currently found at EAR 772.1) and "applied research" (currently found in the DFARS). The preamble suggests that the DFARS definition be used, which is reflected in the ITAR (120.49). It also suggests an alternate definition of applied research taken from OMB Circular A-11: "Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met." Our member institutions are split on this issue. However, universities use the A-11 definition in reporting federal expenditures. Therefore, we suggest that it be adopted. The definition used in the annual NSF Higher Education Research and Development Survey also is very familiar to universities, and would be another good alternative.

4. Whether the questions and answers in existing Supplement no. 1 to part 734 proposed to be removed (to the BIS website) have criteria that should be retained in part 734.

Response: The Q&A's have been very helpful to the universities. They are unlikely to have the same weight if

removed from the EAR and placed on the website. We also note that supplements to other parts of the EAR contain important regulatory information (e.g. Supplement No. 1 to Part 740).

5. With respect to end-to-end encryption as described in the proposed rule (sec. 734.18), whether the illustrative standard in the proposed EAR rule also should be adopted in the ITAR; whether the safe harbor standard in the proposed ITAR rule also should be adopted in the EAR, or whether the two bodies of regulations should have different standards.

Response: We appreciate that the proposed rules address cloud computing situations, which have been an area of considerable uncertainty under the current rules. BIS asks for comments as to which proposed rule more clearly describes the intended control. We prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, we believe that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur. We also prefer the EAR provision in 734.18(4)(iii) providing for "other similarly effective cryptographic means" for securing technology or software. While the NIST standards are widely accepted, not all our members necessarily implement them and may use other means to assure effective cryptographic management.

In addition, the restriction in 734.18(a)(4)(iv) to countries not listed in Country Group D:5 unfortunately may substantially limit the usefulness of the proposed rule. In the experience of our members, most cloud providers insist on storing data anywhere that they want. We suggest BIS consider adding a note that a contract that imposes these obligations on a vendor is sufficient for compliance purposes, to provide a greater safe harbor. Ensuring actual compliance is beyond our members' control.

6. Whether encryption standards adequately address data storage and transmission issues.

Response: Our associations lack the technical expertise to comment on this issue. However, we have encouraged our member institutions to review and provide comments.

7. Whether the proposed definition of "peculiarly responsible" effectively explains how items may be "required" or "specially designed" for particular functions.

Response: these definitions appear reasonable. However, this is another question where we have suggested our member institutions review the application to particular technologies in submitting comments.

8. The effective date of the final rule.

Response: BIS proposes a 30-day delayed effective date. Changes to ECCNs generally have had a six-month delayed effective date while other rules affecting export controls have been effective on the date of publication. Obviously the content of the final rule is an important consideration. Our view is that significant changes in definitions should have as long a lead time as possible for implementation. Therefore we support a six-month delayed effective date.

Conclusion

In closing, we again want to express our appreciation to BIS for their responsiveness to many of the issues and concerns that our members have raised, and your willingness to engage our associations and university

members in dialogue on these issues. We believe the EAR changes are mostly positive and deserving of support. We hope BIS will consider our comments in finalizing the proposed definitions, and are available to provide more information or discuss these matters further.



August 3, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

**Re: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32)
Published in 80 Fed Reg 31505 on June 3, 2015**

Dear Sir/Madam:

On June 3, 2015, the Commerce Department's Bureau of Industry and Security ("BIS") published a Proposed Rule in the Federal Register entitled Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32). See 80 Fed Reg 31505.

The Alliance for Network Security ("ANS") is an industry association comprised of Alcatel-Lucent, Cisco Systems, Inc., Data Direct Networks, Google Inc., Hewlett-Packard Company, Hitachi Data Systems Corp., Intel Corp., Juniper Networks, Inc., Microsoft Corp., Novell, Inc., Qualcomm Inc., Rockwell Automation, Inc. and Symantec Corporation. For over fifteen years, ANS has advised the United States and foreign governments with respect to export and import controls on cryptography. We appreciate this opportunity to provide comments with respect to export controls on definitions that are relevant to the use of cryptography under the Export Administration Regulations (EAR).

The ANS members welcome this opportunity to comment on the Proposed Rule. Our primary interest is in three provisions that, taken together, provide a "safe harbor" for the export of controlled software and technology when used in some "cloud computing" environments (e.g., cloud file storage), including the following provisions in Section 734.18:

- Paragraph (a)(4)(ii), which requires that technology or software be secured using "end-to-end encryption";
- Paragraph (a)(4)(iii), which requires that the technology or software be secured using cryptographic modules compliant with Federal Information Processing Standard 140-2 (FIPS 140-2) or "other similarly effective cryptographic means"; and

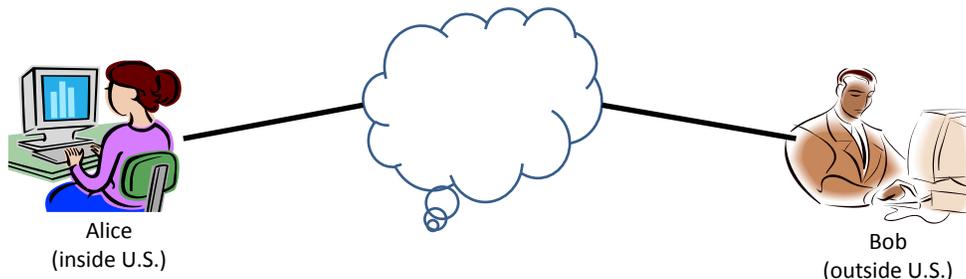
- Paragraph (b), which requires that the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

**The Term “End-to-End” Should be Replaced with
“Security Boundary or End Point-to-Security Boundary or End Point”**

In Paragraph (a)(4)(ii) of Section 734.18, BIS establishes a requirement that information and software must be secured “end-to-end”. We respectfully suggest that the term “end-to-end” should be replaced with “security boundary or end point-to-security boundary or end point”.

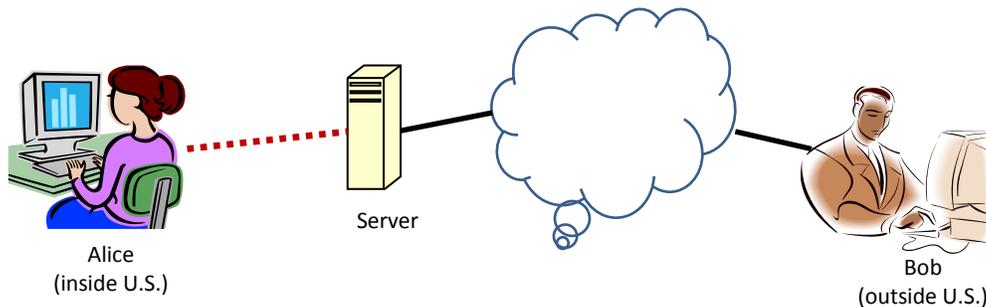
We understand from the preamble to the Proposed Rule that the “intent of this requirement is that relevant technology or software is encrypted by the originator and remain encrypted (and thus not readable) until it is decrypted by its intended recipient.” This requirement is illustrated in Figure 1, where Alice, who is inside the United States, encrypts data on her personal computer or mobile device and sends it to the personal computer or mobile device of Bob, who is outside the United States:

Figure 1: End Point-to-End Point Encryption



However, consider also a second scenario, where Alice is a system administrator of a server which is located inside the United States, and authorizes a download of data to the personal computer or mobile device of Bob, who is outside the United States:

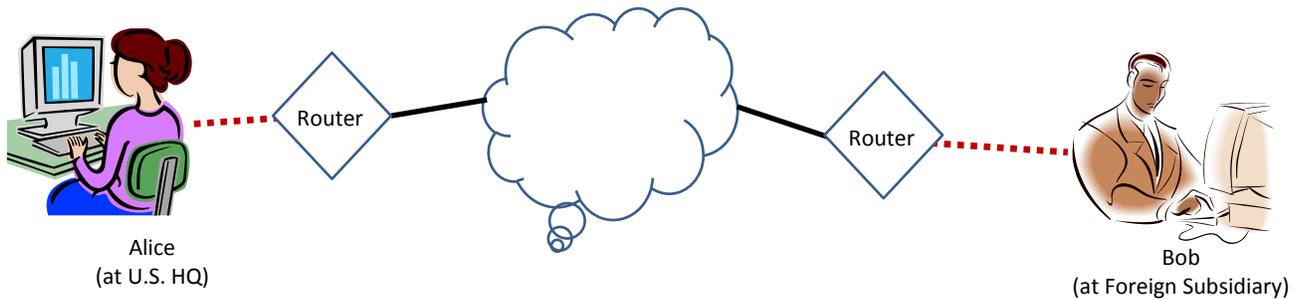
Figure 2: Security Boundary-to-End Point Encryption



Arguably, at the instant of export and until the moment of delivery, the data in transit is equally secure as the data in transit in Figure 1, even though the data in Figure 2 is not encrypted “end-to-end” as we understand that term. (We would refer to this as “security boundary-to-end point” encryption)

Please also consider a third scenario, where Alice is located at the headquarters of a company inside the United States, and Bob is located at the company’s foreign subsidiary outside the United States. In this scenario, the data is encrypted by the edge routers at each office, and the data is sent in encrypted form through a virtual private network:

Figure 3: Security Boundary-to-Security Boundary Encryption



Arguably, at the time of export, the data in transit is equally secure as the data in transit in Figure 1, even though the data in Figure 3 is not encrypted “end-to-end” as we understand that term. Upon receipt, it is equally secure as any other technical data on Bob’s computer or mobile device. The only time when the data is not secured is the brief moment, in transit, within the four walls of Bob’s office. (We would refer to this as “security boundary-to-security boundary” encryption.) Please note that only the transfers of encrypted data data represented by black lines in these three figures would be exempt from the definition of “export”. Transfers of plaintext represented by dotted red lines in figures 2 and 3 would not be exempt from the definition of “export”.

We respectfully suggest that the term “end-to-end” should be replaced by “security boundary or end point-to-security boundary or end point” in the final rule.

The Term “Other Similarly Effective Cryptographic Means” Should Be Replaced with “Other Commercially Reasonable Cryptographic Means”

In Paragraph (a)(4)(iii) of Section 734.18, BIS establishes a requirement that the technology or software be:

Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other

procedures and controls that are in accordance with guidance provided in current U.S. National Institute of Standards and Technology publications, or other similarly effective cryptographic means”.

We respectfully suggest that the term “other similarly effective cryptographic means” should be replaced with “other commercially reasonable cryptographic means”.

As a point of clarification, we think that the phrase “compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors” is not consistent with the terminology used in the Cryptographic Module Validation Program (“CMVP”) for the FIPS 140 logo program. The CMVP validates cryptographic implementations of products according to the current version FIPS 140. The current version is FIPS 140-2. The CMVP Logo only has two options: “FIPS 140-2 Validated” and “FIPS 140-2 Inside”.¹ FIPS 140-2 Validated means that the author of the cryptographic code paid for the validation of the cryptographic module. FIPS 140-2 Inside means that the author of the program is using a cryptographic module that was validated under CMVP by someone else. We think it would be preferable to use these terms in the final rule.

More importantly, in the experience of ANS member companies, a very small number of encrypted transmissions of technology and software actually take place using products that are either “FIPS 140-2 Validated” or “FIPS 140-2 Inside”. The reasons include the facts that: (1) the FIPS algorithm selection² is very narrow, currently including AES, 3DES, ECC, some DH and others, but conspicuously omitting DES, RC2, RC4 and other algorithms in wide commercial use, (2) the FIPS process is voluntary, and can be expensive, and (3) FIPS products generally trail the “state of the art” by months or years, due to the time delays inherent in the FIPS process. An added complication is how ANS member companies and other U.S. Persons are supposed to determine whether a product that has *not* been through the FIPS process is “similarly effective”?

Therefore, we recommend that the term “other similarly effective cryptographic means” be replaced with “other commercially reasonable cryptographic means”. By way of example, cryptographic means used to secure a company’s valuable intellectual property could be used for purposes of meeting the requirement of Paragraph (a)(4)(iii) of Section 734.18.

If we revert to Figure 1, for example, this would authorize the use of PGP as one method of securing emails between Alice and Bob. If we revert to Figure 2, for example, this would authorize the use of implementations of the SSL/TLS protocol for client-server communications between Alice and

¹ <http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPMMPMM.pdf> - see appendixes for details.

² <http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPMMPMM.pdf> - page 44-45 a complete list is found here: <http://csrc.nist.gov/groups/STM/cavp/validation.html> - Included at end for reference.

Bob. If we revert to Figure 3, for example, this would authorize the use of implementations of the IPsec protocol for peer-to-peer communications between Alice and Bob.

**Not Only the Sender and Recipient, but Any Third Party Who is a “U.S. Person”
Should Be Permitted to Manage Keys or Other Means to Access Data in Unencrypted Form**

In Paragraph (b) of Section 734.18, BIS establishes a requirement that the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

This requirement is particularly problematic to Internet service providers, application service providers and cloud service providers, who provide services to U.S. companies. For example, if a software as a service provider does not have access to encryption keys, functionality that requires data analytics such as search, indexing, anti-spam/anti-malware, configurable message transport rules, business intelligence, or issue replication for troubleshooting, may be degraded or rendered non-functional. We see no clear articulation of a rationale which would support exclusion of a business model involving outsourcing of security, including management of keys – provided of course that the Internet service provider, application service provider or cloud service provider itself is a U.S. Person.

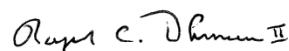
Conclusion

We respectfully recommend that BIS make the following changes in the final rule:

- The Term “End-to-End” Should be Replaced with “Security Boundary or End Point-to-Security Boundary or End-Point”;
- The Term “Other Similarly Effective Cryptographic Means” Should Be Replaced with “Other Commercially Reasonable Cryptographic Means”; and
- Not Only the Sender and Recipient, but Any Third Party Who is a “U.S. Person” Should Be Permitted to Manage Keys or Other Means to Access Data in Unencrypted Form.

Thank you for this opportunity to comment on the Proposed Rule in the Federal Register entitled Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32).

Sincerely,



Roszel C. Thomsen II



ASML US, Inc.

2650 W. Geronimo Place
Chandler, AZ 85224
U.S.A.

www.asml.com

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

and

Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
Bureau of Political Military Affairs
U.S. Department of State
Washington, DC 20522

Via email: publiccomments@bis.doc.gov and
DDTCPublicComments@state.gov

Date	August 3, 2015
Reference	Comments in Response to Proposed Rule Makings
Subject	RIN 0694-AG32 - Revisions to Definitions in the Export Administration Regulations and RIN 1400-AD70 - International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

Ladies and Gentlemen:

ASML US, Inc. ("ASML US") is pleased to respond to the Bureau of Industry and Security ("BIS") and Directorate of Defense Trade Controls ("DDTC") request for comments concerning the proposed revisions to definitions in the Export Administration Regulations ("EAR") and International Traffic in Arms Regulations ("ITAR").

ASML US, headquartered in Chandler, AZ, is a subsidiary of ASML Netherlands, B.V., the world's leading provider of lithography systems to the semiconductor manufacturing industry. ASML US is the parent of Cymer LLC, headquartered in San Diego, CA, the leader in developing light sources used by chipmakers worldwide to pattern advanced semiconductor chips and is pioneering development of next generation light sources.

Rule makings RIN 0694-AG32 and RIN 1400-AD70 propose to:

- (i) revise the EAR to include the definitions of "technology," "required," "peculiarly responsible," "proscribed person," "published," results of "fundamental research," "export," "reexport," "release," "transfer," and "transfer (in-country)" to enhance clarity and consistency with terms also found on the ITAR;
- (ii) amend the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software; and

- (iii) publish comparable amendments to the ITAR's definitions of "technical data," "required," "peculiarly responsible," "public domain," results of "fundamental research," "export," "reexport," "release," and "retransfer" for the same reasons.

ASML US welcomes the U.S. governments stated efforts to enhance U.S. national and economic security, facilitate compliance with export controls, update the controls and reduce unnecessary regulatory burdens on U.S. exporters. With these goals in mind, ASML US has the following comments.

I. Definitions of "Export", "Reexport" and "Release"

A. Inclusion of phrase "otherwise transferring" is confusing

ASML US has some reservations concerning the U.S. government's proposed changes to the definition of "export" and "reexport" under the EAR at § 734.13, which could be interpreted to expand the current understanding of a "deemed export," "deemed reexport" and the "release" of technology. The proposed definition of "export" in § 734.13(a)(2) reads:

Releasing or otherwise transferring "technology" or "source code" (but not "object code") to a foreign national in the United States (a "deemed export");

ASML US believes the inclusion of the phrase "otherwise transferring" within § 734.13(a)(2) is unclear and possibly unnecessary with respect to a "deemed export". "Transfer" is defined in the EAR in the proposed rulemaking as:

Transfer. A shipment, transmission, or release of items subject to the EAR either within the United States or outside the United States.

ASML US is pleased to see that the concept of "release" will be clearly expressed in a new § 734.15. The proposed addition continues to make clear the current understanding that a "release" can occur through (i) visual or other inspection; (ii) oral or written exchanges; or (iii) the application by U.S. persons of "technology" or "software" to situations abroad. However, this understanding seems somewhat at odds with the inclusion of the phrase "otherwise transfer" as it relates to "deemed export" and "deemed reexport". This is because:

- the definition of "transfer" includes the term "release", so adding "otherwise transferring" immediately after "releasing" in § 734.13(a)(2) seems somewhat duplicative; and
- as shown, a "transfer" includes a physical shipment of an item, which has not been relevant to the sharing of information contemplated by "deemed export" or "deemed reexport".

Under a strict reading of the proposed rulemaking, it appears that the mere physical shipment of "technology" or "source code" – for example on physical media such as a flash drive – to a foreign national in the United States would constitute a "deemed export" even if no actual "release" occurs. The inclusion of "otherwise transfer" seems to be an expansion of the current understanding of "deemed export", "deemed reexport" and "release". It is not clear that this is what BIS intends.

In order to avoid confusion, ASML US recommends that the U.S. government remove the phrase "otherwise transferring" from the proposed definitions of "export" and "reexport" as it relates to "deemed export" and "deemed reexport". In the alternative, BIS could use "otherwise transmitting", which seems more appropriate and removes the element of physical export from the definitions.

Date August 3, 2015
Reference Comments in Response to Proposed Rulemakings

ASML US recognizes that BIS is creating a catch-and-release process for the “export”, “reexport” or “transfer” of certain “technology”. That is, BIS is capturing the “transfer” of “technology” or “software” under the definitions of “export” and “reexport” and then releasing those activities which meet the conditions set forth under the proposed § 734.18(a)(4). As a standard matter, ASML US requests that wherever BIS creates a “capture” mechanism in the EAR, that it insert a note in the regulations pointing to the relevant “release” criteria.

B. It is unclear what “software” would be captured under § 734.13(a)(6) and 734.14(a)(4)

ASML is confused by the two uses of “software” in the proposed definitions of “export” and “reexport”, which because they reference a foreign national and not a consignee, appear to be directly related to a “deemed export” and “deemed reexport”. This is also supported by the fact that the proposed definitions use of the phrase “‘*software*,’ or other information”:

§ 734.13(a)(6) Releasing or otherwise transferring [...] “*software*,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “*software*” to a foreign national.

and

§ 734.14(a)(4) Releasing or otherwise transferring outside of the United States [...] “*software*,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “*software*” to a foreign national.

“Software”, writ large and including object code, has not been subject to broad control under the definition of “release”, “deemed export” or “deemed reexport”. Instead the EAR has generally limited a “release” to “source code” as illustrated by the proposed § 734.15(a)(1) and (3):

(1) Visual or other inspection by a foreign national of items that reveals “technology” or “source code” subject to the EAR to a foreign national;

and

(3) The application by U.S. persons of “technology” or “software” to situations abroad using personal knowledge or technical experience acquired in the United States, to the extent that the application reveals to a foreign national “technology” or “source code” subject to the EAR.

(Section 734.15(a)(2) does not appear relevant to “software” or “source code” as it concerns the oral or written exchanges of “technology”.)

ASML US therefore request that the proposed change include clarification concerning what kinds or types of “software” BIS intends to capture through the “release” of “software” that may cause or permit the transfer of other information, “technology” or “software”.

In addition, to avoid confusion, BIS should consider replacing “software” with “source code” as it relates to “deemed exports” and “deemed reexports” or work through the Wassenaar Agreement process to add the particular software applications of concern to the control lists.

As written, the language is so broad that it could capture almost all electronic communication methods such as email, which can be used to transmit information that may cause or permit the transfer of other “technology” in clear text or “*software*” to a foreign national.

Date August 3, 2015
Reference Comments in Response to Proposed Rulemakings

C. Unnecessary expansion of controls over causation and permission

ASML US believes that the addition of the phrase “will cause or permit” in § 734.13(a)(2) is overly broad. By their very nature, decryption keys, network access codes, passwords, etc., permit access to information. The very act of accessing information results in a “release”, which is already a controlled activity. As a result, providing a password with “*knowledge*” that the provision will result in a release of information to a foreign national (which is the very definition of a “deemed export”) just artificially doubles the number of “deemed export” transactions that occur without providing any apparent additional benefit to U.S. national security.

ASML US is additionally very concerned by the BIS’s attempt to control “exports” and “reexports” which only *may* occur, as opposed to actually occurring. The proposed rule would control the provision of a password to an individual even if that password is immediately forgotten, expires and/or is simply never used.

D. Expanding controls on decryption keys and passwords would be burdensome

While ASML US believes it understands BIS’s rationale for attempting to close a potential loophole concerning the release, shipment and transmission of decryption keys and passwords, it finds §§ 734.13(a)(6) and 734.14(a)(4) overly broad and potentially burdensome given that many large companies use identity management (IdM) and/or password automation systems for the generation and maintenance of access codes, passwords, etc.

ASML US, like many technology companies, controls the actual access or “release” of controlled “technology”, not just the distribution of network access codes and passwords. In addition to passwords, ASML US has in place a knowledge protection program and additionally restricts access to protected technology based on, among other things, department affiliation, manager approval and a demonstrated need-to-know. As a result of this layered approach, network access codes and passwords are necessary but not sufficient to gain access to protected information. Because of this layered approach, it is not clear whether the distribution of an access code or password to a foreign national would be sufficient to meet the “will cause or permit” standard.

If the distribution of an access code or password merits control, a company may need to remove certain automated IdM and enterprise resource planning (ERP) systems and use a manual authorization process or, if possible, modify any existing systems and processes to include additional criteria such as, Country Group and license expiration dates. These types of modifications are not made quickly or easily nor are they done at a low cost in terms of money and labor resources.

In addition to these concerns, ASML US has questions concerning how this change is to be applied once a proposed change is promulgated:

- Would all current, valid deemed export and reexport licenses need to be amended to include the transfer of a decryption key, access code, password, etc., as relevant? Or would the control work in the opposite manner, that is, does a validated export license authorizing the transfer of controlled technology to a foreign national automatically authorize access to any relevant decryption key, access code or password?
- Since under the proposed rulemaking, a violation concerning the transfer of decryption keys, network access codes, passwords, etc., would constitute a violation to the same extent as a violation in connection with the export of the controlled “technology” or “software”, how does one classify under the CCL an item such as hardware key fobs or token which allow for two-factor authentication. Currently such hardware is classified on

Date August 3, 2015
Reference Comments in Response to Proposed Rulemakings

the Commerce Control List under Category 5 Part 2, but potentially enables access to technology classified under multiple categories.

- How does one classify a decryption key, access code, password, etc., if it allows access to information or technologies in clear text which are classified under multiple ECCNs?

II. Activities That Are Not Exports, Reexports, Releases, Retransfers or Transfers

A. End-to-end encryption and cloud storage

The proposed § 734.18(a) identifies a number of activities that are not treated as “exports”, “reexports” or “transfers” under the EAR. These activities subject to exclusion include sending, taking, or storing “technology” or “software” that is, among other things, secured using ‘end-to-end encryption.’

While on the face of it, this exclusion from the definition of “export” and “reexport” appears useful, the reality is, it is unlikely to be broadly used. The use of end-to-end encryption greatly restricts what can be done with data that is stored, for example, in a cloud environment. Information, once encrypted, cannot be easily indexed, queried, retrieved or manipulated, which removes much of the utility and benefit from enterprise cloud storage.

Nevertheless, ASML US believes this exclusion is a positive step in the U.S. government’s understanding and treatment of the use of encryption by industry.

B. Activities That Are Not Deemed Reexports

ASML US is very pleased to see BIS promulgate its current guidance concerning “deemed reexports” in the EAR. However, ASML US would like BIS to provide additional clarification in the regulations concerning when the proposed exclusions at § 734.20(a), (b) and (c) are applicable particularly when License Exception Technology and Software Under Restriction (TSR) is available to a foreign national who is either of a country that is identified:

- under Country Group B *and* Country Group A:5 (such as the Netherlands); or
- under Country Group B *and* a country *not* identified under Country Group A:5 (such as Brazil).

Under § 734.20(a), a foreign entity would only need to be certain that the foreign national’s most recent country of citizenship or permanent residency is that of a country to which export from the United States of the “technology” or “source code” at issue would be authorized by, for example License Exception TSR. However, under § 734.20(b) and (c), a foreign entity would need to comply with many additional requirements.

Also, in order to avoid confusion and unnecessary submissions of license applications to BIS, ASML US recommends that a note be inserted in the definition of “deemed reexport” at § 734.14 which point to § 734.20.

Date August 3, 2015
Reference Comments in Response to Proposed Rulemakings

* * *

ASML US greatly appreciates the opportunity to comment on the proposed rulemaking and looks forward to continuing its cooperation with the U.S. government on export control reform.

Sincerely,



Steve Lita
Manager, Export Compliance



August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am writing on behalf of the Association of University Export Control Officers (AUECO), a group of 129 senior export practitioners from 100 accredited institutions of higher learning in the United States (U.S.). AUECO members monitor proposed changes in export control laws and regulations affecting academic activities and advocate for policies, procedures, and award terms and conditions that advance effective university compliance with applicable U.S. export controls and trade sanction regulations.

The proposed Revisions to Definitions in the Export Administration Regulations (EAR) and corresponding changes to the International Traffic in Arms Regulations (ITAR) will, if adopted as proposed, have significant impact on academic institutions in the U.S. We appreciate the opportunity to comment on these revised definitions.

Changes to Educational Information

The current §734.9 defines “educational information” as information released by instruction in catalog courses and associated teaching laboratories of academic institutions, and §734.3(b)(3)(iii) excludes such information from the scope of the EAR. In the proposed rule, the definition of “educational information” is removed, and §734.3(b)(3)(iii) excludes information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution. We believe that the proposed change adds uncertainty and potentially narrows the scope of applicability of the exclusion. Will academic institutions contemplating new curricular additions need to concern themselves that the course may not be commonly taught at other universities? Many catalog courses include hands on design laboratories, particularly as capstone experiences. Does the content of these courses,

which would have previously been treated as “educational information” become subject to the EAR by virtue of including more than general principles?

Universities do not discriminate on the basis of citizenship or national origin in academic programs. Education at universities is by nature open, with the opportunity to participate limited only by required prerequisites. A narrow interpretation of the revised §734.3(b)(3)(iii) would inhibit the ability of U.S. universities to develop new courses in emerging areas of science and engineering critical to employability of their graduates and the future competitiveness of the industrial sector. AUECO recommends that the qualifier “concern general scientific, mathematical, or engineering principles commonly taught in schools” be removed and that the simpler “is released by instruction in catalog courses and associated teaching laboratories of academic institutions” be retained for §734.3(b)(3)(iii). As an alternative, we believe changing the proposed description to “information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and /or released by instruction in a catalog course or associated teaching laboratory of an academic institution” would describe educational information more fully without narrowing the scope of the exclusion.

Definition of “Fundamental Research”

The proposed definition of “fundamental research” using the language of NSDD-189 in the EAR and the ITAR is consistent with U.S. academic institutions’ understanding of the concept. The proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18) with an alternate definition adopting OMB Circular A-11 language.

The OMB Circular A-11 language reads: “applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met”. This language is well understood by universities in the context of reporting on federal expenditures to NSF, and AUECO favors the adoption of this commonly used definition.

We suggest that if the DFARS definition is adopted, the definition of “applied research” would be further clarified by including the rest of 48 CFR part 31.205-18 — “Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development, defined in this subsection.” — the “for sale” criterion will help to clearly distinguish between “applied research” and “development” activities.

BIS has also proposed an alternate definition: “fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. We assume that this simpler definition would not alter other wording in the proposed rule permitting prepublication review under specific circumstances within the fundamental research domain. While we generally favor the simplified definition, it would be helpful if a note were added to illustrate what is and is not non-proprietary, or alternately for the term to be defined. Alternately, AUECO believes that the

ambiguity around the use of the term non-proprietary would be eliminated with another alternate definition.

AUECO suggests using a definition that reads: ““fundamental research” means research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons”. This definition captures the intent of BIS in clear unambiguous language.

AUECO appreciates that the proposed definition of “fundamental research” clarifies the broad applicability of the concept regardless of organization type or location. However, the removal of the specific criteria for university based research currently found in §734.8(b) creates interpretive uncertainty. U.S. universities use §734.8(b) to make determinations as to the applicability of fundamental research by evaluating proposed research activities using paragraphs 2 -6, and assuming that the research qualifies as “fundamental research” if all conditions are met. AUECO recommends that the specific language of §734.8(b) be retained in the EAR. If this is not possible, we suggest that BIS develop a decision tree tool for the determination of fundamental research for universities that incorporates the current criteria for university based fundamental research.

“Fundamental research”, “technology”, and “software” Under the proposed §734.8(a), “technology” that arises during, or results from, fundamental research and is “intended to be published” would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR.

The proposed rule refers to a proposed note “to clarify that software and commodities are not ‘technology resulting from fundamental research’” (although we were unable to locate the note). This change would significantly complicate and restrict university research; while natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions. “Software” resulting from university research is “published” as well as “technology”, as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology. AUECO strongly recommends that the proposed §734.8(a) be revised as follows:

§ 734.8 “Technology” and “software” that arises during, or results from, fundamental research.

(a) “Technology” or “software” that arises during, or results from, fundamental research and is ‘intended to be published’ is not “subject to the EAR.”

(b) Prepublication review. “Technology” or “software” that arises during, or results, from fundamental research is “intended to be published” to the extent that the researchers are free to publish the technology and software source code without

restriction or delay. “Technology” that arises during or results from fundamental research subject to prepublication review is still “intended to be published” when:

Questions and Answers- Technology and Software Subject to the EAR

AUECO urges BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. While we agree that the questions and answers are illustrative, inclusion of them in the EAR removes the uncertainty created by changes due to interpretive differences without benefit of the rulemaking process. We are concerned that removal of the questions and answers, which we use to guide export control decisions at universities, would create increased uncertainty in our application of key concepts including fundamental research, publication, and educational instruction.

End to End Encryption Standard

The addition of §734.18 listing activities that are not exports, reexports or transfers is a useful addition to the EAR. In particular, the exclusion of sending, taking or storing software that is secured using end to end encryption from export activities is welcome to the academic research community as it will reduce the faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. AUECO favors the proposed EAR illustrative standard of FIPS 140-2 supplemented in accordance with NIST guidance or other similarly effective means.

Effective Date of the Final Rule

While the revised definitions do not make changes to the USML or the CCL, as written they have a significant impact on regulatory burden for U.S. universities. Importantly, such review would be required retrospectively for current projects. These procedures will also require additional staffing for export compliance. Universities will not be able to meet the compliance obligations imposed by the proposed changes within 30 days of the publication date. AUECO suggests at minimum a 6 month delay in effective date, and further that the revised regulations be applicable only to new efforts begun after the effective date of the Final Rule.

AUECO appreciates the opportunity to provide comments on these proposed changes.

Sincerely,



Brandi Boniface
Chair
Association of University Export Control Officers
Email: auecogroup@gmail.com
Website: <http://aueco.org>

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th Street and Pennsylvania Ave., N.W.
Room 2099B
Washington, D.C. 20230

Subject: Revisions to Definitions in the Export Administration Regulations

To Whom It May Concern:

SPIE, the international society for optics and photonics, and The Optical Society (OSA) appreciate the opportunity to comment on the proposed changes to the EAR.

SPIE and OSA have some concerns regarding the definition of Fundamental Research as proposed, as follows:

(c) *Fundamental research definition.* “Fundamental research” means basic or applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. This is distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.

In order to fully encompass the research community, we recommend that the reference to “science and engineering,” in the first sentence be changed to “science or engineering”.

We also recommend that the language stating “published and shared broadly within the scientific community” in the first sentence be changed to “published and shared broadly within the research community.”

Furthermore, the EAR proposed changes include definitions of “basic research” (734.8, EAR 772.1) and “applied research” (based on DFARS; the ITAR (120.49)).

(1) *Basic research* means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

2) “Applied research” means the effort that:

- (i) Normally follows basic research, but may not be severable from the related basic research;
- (ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques; and
- (iii) Attempts to advance the state of the art.

These definitions create issues for certain basic and applied research, such as validation research and requiring that applied research be tied to basic research. As an alternative, we recommend using the National Science Foundation definitions, as follows:

- Basic research: systematic study to gain knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications toward processes or products in mind;
- Applied research: systematic study to gain knowledge or understanding necessary for determining the means by which a recognized and specific need may be met;

Thank you for your consideration of these concerns. Please contact us for any additional information.

Sincerely,

Eugene Arthurs
CEO
SPIE

Elizabeth Rogan
CEO
The Optical Society

SPIE is the largest international not-for-profit society in optics, photonics and imaging. Together with our 18,000 individual members and 600 corporate members, the Society seeks to build a better world with light through scientific education and innovation.

Founded in 1916, OSA is home to accomplished science, engineering, and business leaders from all over the world. Through world-renowned publications, meetings, and membership programs, OSA provides quality information and inspiring interactions that power achievements in the science of light. OSA represents over 19,000 individual members and 265 businesses. OSA's mission is to promote the generation, application and archiving of knowledge in optics and photonics and to disseminate this knowledge worldwide.

K&L GATES

K&L GATES LLP

1601 K STREET, N.W.

WASHINGTON, DC 20006

T +1 202 778 9000 F +1 202 778 9100 klgates.com

August 3, 2015

Daniel J. Gerkin
daniel.gerkin@klgates.com

T 202.778.9168

F 202.778.9100

VIA ELECTRONIC MAIL

Hillary Hess
Director
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, N.W.
Washington, DC 20230

Re: RIN 0694-AG32 - Revisions to Definitions in the Export Administration Regulations

Dear Ms. Hess:

On behalf of our client, Kaman Corporation (“Kaman”), we provide the following comments on the amendment proposed by the Bureau of Industry and Security of the U.S. Department of Commerce (“BIS”) to the Export Administration Regulations (“EAR”; 15 C.F.R. part 730 *et seq.*) to, among other changes, add Section 734.18, Activities that are not exports, reexports, or transfers. *See* 80 Fed. Reg. 31505, at 31517 (June 3, 2015). Proposed Section 734.18 provides in part, under paragraph (a), that “The following activities are not exports, reexports, or transfers: ... (4) Sending, taking or storing technical data or software that is ... secured using end-to-end encryption ... and [n]ot stored in a country listed in Country Group

D:5...” Presumably, this proposed provision is intended to update the EAR to take into account current technical data storage and transfer technologies and practices, including the potential for utilization by persons in the United States of non-U.S. based cloud computing and/or remote offshore servers to electronically store technical data and/or transfer communications, such as emails, that may contain technical data.

Similarly, U.S.-based electronic storage and/or transfer devices potentially could be utilized by persons outside the United States in connection with cloud computing and/or the storage of non-U.S. technical data and/or the electronic transfer of communications containing non-U.S. technical data, such as through email. Accordingly, we believe that, assuming Section 734.18 ultimately is adopted as part of the EAR, it also should clarify that the electronic storage and/or transfer of non-U.S. origin technical data by non-U.S. persons using electronic storage and/or transfer devices located in the United States, and the subsequent transfer and/or retrieval of that technical data by non-U.S. persons, does not result in an import or an export and also are “[a]ctivities that are not exports, reexports, or transfers” under the EAR.

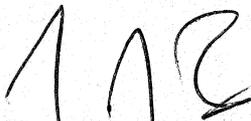
Unlike the storage or transfer of U.S.-origin technical data outside the United States by U.S. persons, which under proposed Section 734.18 must include end-to-end encryption to not constitute an export, we believe that such encryption should not be required in the case of non-U.S. origin technical data stored and/or transferred in the United States by non-U.S. persons. Simply, the same U.S. export control policy considerations do not apply. But for the use of data storage/transfer services in the United States, such technical data could not become subject to the EAR and, because the use of the U.S. data services would not in any way affect the composition of the technical data and the services presumably would have no role in dictating or controlling

the retrieval and/or transfer of the technical data, there is no policy basis for imposing EAR controls on such technical data. Likewise, access to the technical data by U.S.-based IT personnel in the course of maintaining the function and integrity of the storage/transfer devices, and/or the periodic transfer of technical data from the devices to any U.S. persons, should not affect the applicability of EAR controls, except that such controls presumably would apply to any “copy” of the technical data received by a U.S. person (but not to the data as placed by the non-U.S. person and residing on the storage device).

Alternatively, BIS could adopt a provision relating to the storage and/or transfer in the United States of technical data by non-U.S. persons that parallels paragraph (4)(ii) of proposed Section 734.18 , in effect providing that technical data transferred into the United States by a non-U.S. person and retrieved/transferred out of the United States, secured using end-to-end encryption, would not be considered imported into or exported from the United States. As noted above, however, access by U.S.-based IT personnel for the purpose of maintaining the function and integrity of the storage/transfer devices and/or the periodic transfer of technical data from the devices to any U.S. persons, should not affect the applicability of EAR controls, except that such controls presumably would apply to any “copy” of the technical data received by a U.S. person in unencrypted form (but not to the data as placed by the non-U.S. person and residing on the storage device).

Kaman appreciates this opportunity to provide comments on BIS’s proposed amendments to the EAR.

Respectfully submitted,



Daniel J. Gerkin
Jerome J. Zaucha

Counsel to Kaman Corporation



BROWN

DAVID A. SAVITZ, PhD
Vice President for Research

August 3, 2015

Ms. Hillary Hess, Director
Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

By email to: publiccomments@bis.doc.gov

Subject: RIN 0694-AG32, Revisions to Definitions in the Export Administration Regulations

Dear Ms. Hess:

On behalf of Brown University (Brown), I appreciate the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*. We appreciate the efforts of the Departments of Commerce, Defense, and State to reform, clarify, and harmonize U.S. export control regulations.

Brown fully endorses the comprehensive response to these proposed reforms that have been submitted by the Council on Governmental Relations (COGR) and the Association of American Universities (AAU). Brown University has been in contact with our colleagues at COGR and AAU and we offer our support for the analysis, comments and recommendations made by these associations. We limit our own specific comments to a few matters that are of great importance to Brown in support of our mission.

Alternate definition of “fundamental research” (§734.8(c))

Brown supports BIS’ efforts to provide an alternate definition of “fundamental research” and appreciates that the proposed definition offers some clarity for universities and remains consistent with NSDD-189. We offer the following suggestions related to the proposed definition:

1. We are concerned that the new definition includes the undefined term “non-proprietary” to qualify the type of research that meets this definition. Brown interprets “non-proprietary” to mean research for which the institution or its researchers *have not accepted restrictions for proprietary or national security reasons*. Therefore, Brown proposes alternative wording which we believe is consistent with the intent of the proposed revision: “Fundamental research’ means

research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, *and for which the institution and its researchers have not accepted restrictions for proprietary or national security reasons.*”

2. While we appreciate that the proposed definition of “fundamental research” clarifies its broad applicability regardless of organization type or location, U.S. universities, like Brown, have found the specific criteria for “University based research” (current at §734.8(b) and specifically ¶ 2 – 6) invaluable in evaluating whether proposed research meets the definition of “fundamental research”. We recommend that the specific language of §734.8(b) be retained in the EAR to enable universities to continue to make reliable self-assessments.

3. Finally, we raise a general concern that this proposed alternate definition of a term that is critical to Brown – “fundamental research” – in the EAR creates a unique definition of a term that is shared across the EAR and the International Traffic in Arms Regulations (ITAR) without implementing this same revision in the ITAR. Brown proposes that the changes to this and other common definitions be implemented simultaneously in both sets of regulations to adhere to the stated goals of harmonizing terms to minimize confusion and ease the burden of compliance.

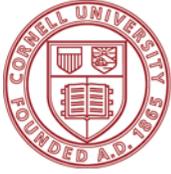
Questions and Answers - Technology and Software Subject to the EAR

Brown University urges BIS to retain the questions and answers found in Supplement No. 1 to part §734 in the regulations. While we agree that the questions and answers are illustrative, inclusion of them in the EAR removes uncertainty created by the subtle nuances of fundamental research and is extremely helpful in clarifying and understanding the EAR. We are concerned that removal of the questions and answers, which we use to guide export control decisions at universities, would create increased uncertainty in our application of key concepts including fundamental research, publication, attendance at conferences and educational instruction.

Sincerely,



David A. Savitz, PhD
Vice President for Research



Cornell University

Office of the Vice Provost
for Research

Robert A. Buhrman

*Senior Vice Provost for Research
Vice President for Technology Transfer,
Intellectual Property and Research Policy
John Edson Sweet Professor*

222 Day Hall

Ithaca, New York 14853-2801

t. 607.255.7200

f. 607.255.9030

rab8@cornell.edu

August 3, 2015

Regulatory Policy Division

Bureau of Industry and Security

U.S. Department of Commerce

By email to publiccomments@bis.doc.gov

Subject: RIN 0694-AG32 - Cornell University Comments

To Whom It May Concern:

Cornell University is committed to its mission of supporting fundamental research that fosters and encourages the free and open exchange of cutting edge ideas and advancements. We appreciate the opportunity to comment on the proposed revisions to the Export Administration Regulations, so that this mission, which is consistent across institutions of higher learning, can be maintained in a way that also protects our nation's interests in export control.

Cornell University offers the following comments:

Educational Information

Cornell University is particularly concerned with the proposed restatement of the "education exemption" in the current EAR 734.9, which is removed and reserved. The new statement in the proposed EAR 734.3(b)(3)(iii) merges current ITAR (120.10(b)) and EAR text to state "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution."

A narrow interpretation of this proposed definition could limit this exemption to only "general principles" and ones that are "commonly taught." At Cornell University, we take pride in a curriculum that offers education in original, innovative and progressive fields.

We recommend removing the phrase "concern general scientific, mathematical, or engineering principles commonly taught in schools" and further recommend that the current "released by instruction in catalog courses and associated teaching laboratories of academic institutions" be retained for proposed EAR 734.3(b)(3)(iii). Alternatively, we suggest that the "and" be changed to "and/or" to avoid limiting this section completely.

Fundamental Research

Cornell University has only one concern with the proposed revision of Fundamental Research. Our concern centers on the vagueness in the term "non-proprietary" as it reads in the proposed new definition. We therefore propose the following: "Fundamental research' means research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons."

Cornell University also recommends that the current presumption that university based research be considered fundamental research, be included in the final rule. The presumption has offered clarity to many universities and we have noted with concern that it has been eliminated from the proposed rule.

Technology and Software

Currently EAR (734.3(b)(3)), states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. Under the proposed revision, technology arising during or resulting from, fundamental research, with the intent to be published, is not subject to the EAR. However, the exclusion for software is removed. This change would significantly complicate and restrict university research.

Cornell University notes that the proposed definition would exclude natural-language documents written by a researcher; however a computer-language document (a program in source code) written for the same project, would be subject to export restrictions. "Software" resulting from university research is "published" as well as "technology", as recognized in the current EAR 734.7(b). The export definitions in 734.2(b) recognize the similarities between software and technology. We strongly recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.

Excluding the sending, taking or storing of technology or software that is secured using end-to-end encryption from control as exports is welcome to the academic research community.

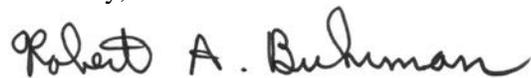
Final Rule Effective Date

The proposed changes could have a significant impact on research activities at Cornell University and could require substantial changes to our current practices. While the final content is a major factor, Cornell University encourages and supports a minimum six month delayed effective date. We believe this is consistent with the delay implemented when significant changes have been implemented in the past.

Other Comments

Cornell University has reviewed comments being submitted by the Council on Governmental Relations (COGR) and the Association of American Universities (AAU) regarding the proposed changes to the export regulations. The issues outlined above are of particular significance; however where we have not commented, Cornell University is likewise in agreement with the comments of COGR and AAU.

Sincerely,



Robert A. Buhrman
Vice President for Technology Transfer, Intellectual Property and Research Policy
Senior Vice Provost for Research



INDIANA UNIVERSITY

OFFICE OF THE VICE PRESIDENT FOR RESEARCH

August 3, 2015

Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, DC 20230
publiccomments@bis.doc.gov

RE: RIN 0694-AG32

To Whom It May Concern:

Indiana University (IU) is a public research institution with a mission to provide broad access to education for students throughout Indiana, the United States, and the world. As a leading research institution and member of the Association of American Universities (“AAU”) and Council on Governmental Relations (“COGR”), IU writes to endorse the comments submitted by these organizations regarding the proposed revisions to the Export Administration Regulations (RIN 0694-AG32) and the proposed amendments to the International Traffic in Arms Regulations (RIN 1400-AD70).

IU is committed to complying with all legal obligations, including export control laws. We appreciate the recent efforts made in export control reform. Harmonized definitions are a very important step of export control reform because they help clarify and streamline compliance obligations for industry and academia; however, some of the proposed changes require additional clarification and modifications to reach this goal and to be consistent with the intent behind the proposals.

First, IU shares the COGR and AAU concern over the restatement of the educational exclusion (currently in §734.9 and proposed to be moved to § 734.3(b)(3)). The preamble indicates that the change “is not intended to change the scope of the current § 734.9 *Revisions to Definitions in the Export Administration Regulations*, 80 Fed. Reg. 31505, 31507 (June 3, 2015); however, the new definition in §734.3(b)(3)(iii) adds qualifiers to the existing scope of the definition. The proposed rule uses “and” to join the new phrase “that...concern general scientific, mathematical, or engineering principles commonly taught in schools” with the existing standard “released by instruction in a catalog course or associated teaching laboratory of an academic institution...” This potentially limits the exclusion. BIS should consider retaining the existing language without change or using “or” to join these phrases instead of “and.”

Second, IU has concerns over the changes to § 734.3(b)(3) and §734.8. Currently § 734.3(b)(3)(ii) excludes from the EAR technology and software that arise during, or result from, fundamental research. The proposed §734.8(a) indicates that only technology that arises during, or results from, fundamental research and is intended to be published, is not subject to the EAR. The preamble to the proposed rulemaking includes a comment that software is not technology resulting from fundamental research (though the note mentioned in the preamble does not seem to be included in the proposed § 734.8). The proposed § 734.3(b)(3) still indicates that information and software arising during, or resulting from,

August 3, 2015
Regulatory Policy Division, Bureau of Industry and Security
RE: RIN 0694-AG32
Page 2

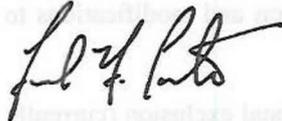
fundamental research, are excluded from the EAR, but the seemingly inconsistent language in both the proposed § 734.8 and note in the preamble will create confusion. IU recommends that BIS resolves the potential conflict in favor of the language in § 734.3(b)(3)(ii) so that software arising during, or resulting from, fundamental research, is clearly not subject to the EAR.

Similarly, IU is also concerned that the presumption that university-based research will be fundamental research, has been eliminated from the definitions. Currently § 734.8(b)(1) states research conducted at a university normally will be considered fundamental research, and the definition of "University" in parentheses at the end of § 734.8(b)(1) clarifies that university means any accredited institution of higher education located in the United States. IU requests that BIS add the current presumption back into § 734.8 in the final rule.

Finally, BIS asked whether the questions and answers in existing Supplement No. 1 to Part 734, proposed to be removed, have criteria that should be retained in Part 734. IU believes that the supplement itself should remain in Part 734. The additional information has been very useful to IU and many other universities, and the questions and answers would not have the same weight on a standalone webpage as they do in the supplement to Part 734.

We are happy to expand on these comments or provide any additional information you might require. Thank you for the opportunity to respond to the proposed rulemaking.

Respectfully,



Fred. H. Cate
Vice President for Research
Indiana University



August 3, 2015

Ms. Hillary Hess, Director
Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security
Department of Commerce
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Subject: RIN 0694-AG32, Revisions to Definitions in the Export Administration Regulations

Reference: Federal Register/ Vol. 80, No. 106/ Wednesday, June 3, 2015/ Proposed Rules

Dear Ms. Hess,

The Boeing Company (“Boeing”) appreciates the opportunity to provide comments to the Bureau of Industry and Security’s (“BIS”) Proposed Rule on definitions in the Export Administration Regulations (“EAR”). Clear definitions are critical for understanding regulatory requirements so we applaud the effort by BIS and the Directorate of Defense Trade Controls to both clarify and harmonize definitions in the EAR and the International Traffic in Arms Regulations (“ITAR”). Updated definitions and clarifying notes will facilitate accurate interpretations and strengthen compliance.

BIS states that most of the proposed changes seek merely to clarify and update definitions without impacting scope. Boeing does perceive scope change in some areas discussed below which are potentially very significant. This Proposed Rule covers areas that are key to determining export requirements. We have endeavored to work through scenarios and consider potential impacts during the sixty day comment period. Given the breadth of the proposed changes, Boeing recommends that definitions change be issued in an Interim Final Basis with at least 60 days to submit additional comments.

There are many welcome changes in these proposed definitions. We’d like to specifically thank BIS for proposed amendments to the scope sections of the EAR to update and clarify the application of controls on electronically transmitted and stored technology and software. At Boeing we believe this will enable industry to apply a wider range of international network and data storage solutions, reducing cost and compliance risk.



Additional positive developments:

- The proposed note to 743.3(b)(3) that distinguishes information from “technology”;
- Addressing internet postings in 734.7(a)(4);
- Replacing “software” with “source code” in 734.13;
- Numerous small changes to “release” in §734.2(b)(3) that increase clarity, for example using “source code” instead of “software”, adding “subject to the EAR”, and clarifying that “technology” must be revealed to have “release”;
- Deleting the reference to specific CCL categories in the definition of “required”; that reference led to mistaken assumptions that the “required” concept did not apply to all “technology” ECCNs, which it does as confirmed in the March 25, 2014 Advisory Opinion;
- Incorporating the permanent employee Advisory Opinion Guidance into §734.20.

Areas where we have questions or recommendations are detailed below.

1. Not Subject to the EAR, §734.3 (b)(3)

The proposed Note to paragraph (b)(3): “*Except as set forth in part 760 of this title, information that is not within the scope of the definition of “technology” (see § 772.1 of the EAR) is not subject to the EAR*” is a helpful addition. Given this note, however, it is confusing that the term “information” is used in the text of the control instead of “technology”: “(b) The following items are not subject to the EAR: (3) **Information** and “software” that: ...” (emphasis added). Clarification is required whether “information” is used because Part 760, *Restrictive Trade Practices, or Boycotts*, controls information that does not meet the definition of “technology”.

2. §734.7 Published

Boeing notes the slight change in wording regarding placement in libraries. The current wording is “Ready availability at libraries open to the public or at university libraries.” The proposed text, shown below, refers to libraries “that are open and available to the public”. The term “open” now applies to university libraries – but many of these have entry controls requiring a student or faculty badge for safety reasons. Clarification is required whether such university libraries would still qualify as “open to the public”.

3. §734.13 Export

▪ Services under the EAR

It is a longstanding principle of the EAR that services are not *per se* exports, rather one must consider whether such services involve a transfer of “technology”. Defense services are exports in the ITAR as stated in §120.17 Export, section (a)(5). This difference can be confusing for exporters that previously dealt only with the ITAR. Boeing recommends that the

BIS principle be added to the regulations in §734.13(a)(5), which is the EAR counterpart to §120.17(a)(5). The proposed language below tracks the ITAR language:

§734.13(a)(5) Performing a service, on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad, is not *per se* an export under the EAR, unless such service involves release of “technology” or “software”, as described in §734.15.

- Permanent residents and protected individuals

The reference to permanent residents and protected individuals, which is in the current regulatory text at 734.2(b)(2)(ii), was not included in 734.13(a)(6), which deals with the release of decryption keys to foreign nationals in the United States. The reference does appear in the counterpart to this section, 734.18(a)(2), *Activities that are not export, reexports, or transfers*. For consistency Boeing recommends including the reference (bolded and underlined below) in both the section describing what is an export (734.13) and the section describing what is not an export (734.18).

§ 734.13(a)(6), Releasing or otherwise transferring decryption keys, network access codes, passwords, “software,” or other information with “knowledge” that such provision will cause or permit the transfer of other “technology” in clear text or “software” to a foreign national. **This does not apply to persons lawfully admitted for permanent residence in the United States and does not apply to persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).**

4. **§734.13 (a)(6) Clear Text and Release of Decryption Keys, etc.**

- Clear text definition

BIS requested input on whether a specific EAR definition of the term “clear text” is warranted. Boeing does recommend including a definition for this term in Part 772 and finds the one cited in the Proposed Rule acceptable, namely:

772.1 Clear text means information or software that is readable without any additional processing and is not encrypted.

- Release of decryption keys

BIS also seeks comments on whether the EAR or ITAR formulations are more clear for release of decryption keys, passwords etc. Boeing notes the different standards for release in the two regulations as a potential area for future discussions amongst the agencies. Our comments are limited to maximizing the alignment of words in the two formulations as follows:

EAR §734.13(a)(6) Releasing or otherwise transferring decryption keys, network access codes, passwords, “software,” or other information, or providing physical access with “knowledge” that such provision will cause or permit the transfer of other “technology” in “clear text” or “software” to a foreign national.

ITAR §120.17(a)(6) Releasing or otherwise transferring ~~information such as~~ decryption keys, network access codes, passwords, ~~or~~ software, or other information, or providing ~~or~~ physical access that would allow access to other technical data in clear text or software to a foreign person regardless of whether such data has been or will be transferred; or

5. §734.14 Reexport

The term “deemed reexport” is defined in subparagraph (2) of this section, and is also critical to understanding §734.20, *Activities that are not “deemed exports”*. Given its importance, Boeing recommends including the definition of “deemed reexport” in Part 772 with other EAR definitions.

6. §734.16 Transfer (in country)

The proposed text, shown below, implies that a change in end use by the same end user constitutes a transfer (in country) for which, presumably, a new authorization is required. That is not the plain meaning of the current text: “The shipment, transmission, or release of items subject to the EAR **from one person to another person** that occurs outside the United States within a single foreign country” (emphasis added). The proposed text therefore appears to be an expansion of scope. Boeing recommends the following revision:

§734.16 Transfer (in country) Except as set forth in §734.18, a transfer (in-country) is a change in end use or end user of an item from one person to another person within the same foreign country.

7. §772.1 “Technology”

- General Technology Note and “required”

Boeing is concerned by the removal of references to the General Technology Note (“GTN”)¹ in the proposed definition. The GTN is referenced in Wassenaar Arrangement definition of technology:

“Technology”

¹ Supplement 2 to Part 744: *General Technology Note*. The export of “technology” that is “required” for the “development”, “production”, or “use” of items on the Commerce Control List is controlled according to the provisions in each Category. “Technology” “required” for the “development”, “production”, or “use” of a controlled product remains controlled even when applicable to a product controlled at a lower level.

*Specific information necessary for the "development", "production" or "use" of a product. The information takes the form of 'technical data' or 'technical assistance'. Controlled "technology" for the Dual-Use List is defined in the **General Technology Note** and in the Dual-Use List. Controlled "technology" for the Munitions List is specified in ML22. (emphasis added).*

The GTN contains the "required" concept which is critical for analyzing export requirements. Reference to the GTN or use of the term "required" is not consistent in ECCNs. BIS confirmed in its response to an Advisory Opinion on March 25, 2014 (posted on the BIS website), that "the GTN and the EAR's definition of "required" apply to all references to "technology" in all the ECCNs on the CCL." Accordingly, it is critical to maintain the *Nota Bene* which references the GTN in the "technology" definition, which reads as follows:

N.B.: Controlled "technology" is defined in the General Technology Note and in the Commerce Control List (Supplement No. 1 to part 774 of the EAR).

An alternative means of incorporating the "required" concept into the "technology" definition would be to replace the word "necessary", as currently used, with the word "required". This would harmonize with the proposed ITAR definition, but would not align with the Wassenaar Arrangement definition.

- Note 2 regarding EAR99 "technology"

In addition, Note 2 of the existing definition is also removed as a proposed change. Boeing recommends retaining this note as it provides helpful clarity for how to treat "technology" that is not controlled by a listed ECCN. The existing note reads as follows:

Note 2: "Technology" not elsewhere specified on the CCL is designated as EAR99, unless the "technology" is subject to the exclusive jurisdiction of another U.S. Government agency (see § 734.3(b)(1)) or is otherwise not subject to the EAR (see § 734.4(b)(2) and (b)(3) and §§ 734.7 through 734.11 of the EAR).

- Elements of "use"

In the Supplementary Information, BIS states that the rulemaking does not propose to change BIS's long standing policy that all six activities in the definition of "use" be present for an item to be classified under an ECCN paragraph that uses "use" in quotation marks. BIS has stressed in outreach programs that elements of "use" are controlled when they are listed without quotation marks or individually as with most 600 Series ECCNs. Boeing strongly recommends adding a Note to the "technology" definition that clearly states this important principle. Our recommendation below is based on BIS's statement in the Supplementary Information:

Note: All six activities in the definition of "use" (operation, installation (including on-site installation), maintenance (checking), repair, overhaul and refurbishing) must be

present for an item to be classified under an ECCN paragraph that uses “use” in quotation marks to describe the technology controlled.

8. 772.1 Peculiarly responsible

Boeing is very concerned with the proposed definition of “peculiarly responsible” which borrows the “specially designed” catch and release construct. Under the proposal, all technology peculiar to the “the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item” is initially caught, even if they are not responsible for achieving the controlled performance levels, characteristics or functions. Such technologies would not be considered to be even potentially covered by “required” under the existing text. Furthermore, the releases, borrowed from the “specially designed” definition, do not release the proper technologies from control.

A hypothetical example would be a technology for application of sizing to a carbon fiber satisfying the performance levels of 1C010.b. The sizing does not have any bearing on the fiber properties in the control listing and therefore is not “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions”. This technology would not get picked up by the existing definition. However, under the proposed rule, because the sizing is used in the production of an item subject to the EAR, it is considered to be “peculiarly responsible” and “required” unless one of the exclusions apply. If none of the exclusions do apply, then the sizing gets “caught”.

This represents an abandonment of the concept of “peculiarly responsible for achieving the controlled performance levels and functions” and moves the control scope to “peculiar to a controlled item”. Boeing believes this to be a far reaching change of philosophy with potentially large licensing impacts. Moreover, the term is not defined in the Wassenaar Arrangement thus potentially leading to an unlevel playing field for U.S. companies.

The production technologies example in the current definition is sufficient to illustrate the meaning of “peculiarly responsible”. Boeing recommends that BIS not provide a separate definition for this embedded concept, but rather clarify the existing definition as follows:

§772.1 “*Required*”. (General Technology Note)—

As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such “required” “technology” or “software” may be shared by different products. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not ~~“required” to produce~~ **peculiarly responsible for producing** the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are ~~“required” to make~~ **peculiarly responsible for making** the controlled product and are themselves



“required” and therefore controlled under the General Technology Note. (See the General Technology Note.) (emphasis added)

9. §734.20 Activities that are not “deemed reexports”

- Non-U.S. entity obligation for deemed reexport compliance

BIS states that this section merely codifies BIS’s interagency-cleared Deemed Reexport Guidance posted on the BIS website. Boeing agrees that the substance of that Guidance is now in 734.20, but the Advisory Opinion was clearly addressed to entities outside the United States with this language: “In general, **you (e.g. an entity outside the United States)** may reexport technology or source code subject to the EAR outside the United States to a dual or third country national without an additional license issued by BIS or the application of an EAR license exception....” (emphasis added). The text in 734.20 does not contain this clarification, which could lead U.S. exporters to believe that they must screen the employees of all recipient companies, even when exporting under an exception or when no license is required. Boeing recommends revising the text as follows to address this:

§ 734.20 Activities **by non-U.S. entities** that are not “deemed reexports.”

- Territory limitation

With regard to the proposed language in Part 734.20(b), Boeing offers that if a foreign national can receive “technology” or “software” at their office in a Country Group A:5 country, then they should be able to receive the same “technology” when abroad, for example at meetings or while on business travel. Boeing recommends deleting subparagraph (b)(4) or at a minimum revising it to also include countries where the entity conducts official business or operates, which is part of 734.20(c) Release to other than A:5 nationals.

Thank you for the opportunity to provide comments. Please do not hesitate to contact me if you have any questions or need additional information. I can be reached at 703-465-3505 or via email at christopher.e.haave@boeing.com.

Sincerely,

Christopher Haave
Director, Global Trade Controls

From: Lisa Palazzo <lxp66@case.edu>
Sent: Monday, August 03, 2015 2:38 PM
To: PublicComments
Subject: RIN 0694-AG32

Good afternoon.

I am writing to express Case Western Reserve University's support of the comment letters sent to you by the Association of American Universities (AAU), Council on Governmental Relations (COGR), and the Association of Export Control Officers (AUECO) regarding proposed revisions to the federal export control regulations.

Kind regards,

Lisa Palazzo, JD

Director of Export Control and Privacy Management

Case Western Reserve University

phone: 216.368.5791 <tel:216.368.5791>

email: lisa.palazzo@case.edu <mailto:lisa.palazzo@case.edu>

web: <http://www.case.edu/compliance/exportcontrol/>
<<http://www.case.edu/compliance/exportcontrol/>>

10900 Euclid Avenue Cleveland, OH 44106-7020

Visitors & deliveries: 2040 Adelbert Road, Suite 311



The Chemours Company
1007 Market Street
PO Box 2047
Wilmington, DE 19899

302-773-1000 t
chemours.com

August 3, 2015

VIA ELECTRONIC MAIL

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce, Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, D.C. 20230

Re: Revisions to Definitions in the Export Administration Regulations; RIN 0694–AG32

To whom it may concern:

The Chemours Company appreciates the opportunity to submit comments regarding the proposed Revisions to Definitions in the Export Administration Regulations published in the June 3, 2015, Federal Register. The proposed changes seek to “enhance clarity and ensure consistency” with the ITAR. While Chemours supports efforts to harmonize and streamline the regulations, we are particularly concerned about sections 734.13(6), 734.18(a)(4), 734.18(b), and 734.18(c). These sections outline the conditions which make (or do not make) a transfer of technical data or information an export by means of Information Technology (IT) systems requiring access codes, passwords, etc. We caution that the proposed changes to these sections would cause significant resource and financial burden on industry.

A. Proposed Change to §734.13(6)

The proposed language of this section provides:

“(6) Releasing or otherwise transferring decryption keys, network access codes, passwords, ‘software’ or other information with ‘knowledge’ that such provision will cause or permit the transfer of other ‘technology’ in clear text or “software” to a foreign national.”

Our interpretation of the text as written is that, after releasing decryption keys, network access codes, passwords, etc., the mere possession of the decryption keys, network access codes, passwords, etc., would not necessarily “cause” a transfer of technology in clear text to a foreign national. However, possession of the decryption keys, network access codes, passwords, etc., would “*permit*” a transfer of technology in clear text to a foreign national despite the owner of the technical data specifically prohibiting their use and access.

Proposed §734.13(6) would severely limit the industry practice of offshore outsourcing of computer systems management and is contrary to current BIS guidance. Current BIS guidance allows computer systems to be managed by restricted foreign nationals provided they do not access and read the files stored in the computer systems. This restriction is customarily a requirement of the service contract with the service provider and the activities performed by IT specialists are monitored or tracked. Additionally, because some information is also business confidential, there are business reasons to have the appropriate contractual terms denying access to files and to strictly enforce compliance with those terms.

Moreover, at a BIS webinar on June 10, 2015, it was stated that proposed §734.13(6) is not a change to BIS guidance and policy regarding foreign computer system management. However, the proposed language does describe a departure from current BIS guidance. If BIS intends to retain the current policy, we suggest that the phrase, “or permit” be omitted from the proposed text of §734.13(6).

B. Encryption in §734.18(a)(4), §734.18(b), and §734.18(c)

These sections describe “end-to-end” encryption as an acceptable way to transmit technical data without creating an export. Encryption of documents poses significant challenges for industry. Maintaining encryption capability adds the required task and expense of maintaining encryption certificates, including tracking expiration dates, funding new certificates and running the implementation process, which may include coordinated testing internally and with business partners to ensure access is not compromised.

Software that generates documents (e.g., Microsoft Word, Microsoft Excel, etc.) are constantly being upgraded and changed by the developer. After several software versions, the encryption keys are incompatible with the document and the document can no longer be accessed. Additionally, when a company is sold or merges with another company, the encryption keys for the company are changed. Again, documents previously encrypted become inaccessible.

If the primary concern is the security of technical data associated with “600 series” items, we submit that encryption should be limited to that particular technical data and not be applied to the entire EAR.

C. Implementation Implications of §734.13(6)

There would be two ways to implement §734.13(6) as written: encryption or separation of controlled technical data into computer systems managed by nationals who fulfill NLR requirements for the control level of the technical data. Some of the encryption issues have been discussed above in Section B. In addition, because encryption would have to be manually applied to each document, retrofitting encryption to documents already stored in computer systems managed by restricted foreign nationals would be a mammoth undertaking due to the massive number documents. Thus, separation of technical data into a separately managed computer system is the only practical way to comply with §734.13(6) as proposed.

Such separation of computer systems would be costly to implement and maintain. Without greater detail regarding programming requirements, we roughly estimate that costs to analyze, create separate computer domains, and move technical data to the correct domain, to be in the tens of thousands of dollars and possibly over one hundred thousand dollars. Additional significant costs will be incurred with the maintenance of separate systems staffed by U.S. or EU personnel. It will roughly increase computer systems costs by 3 to 5 times or hundreds of thousands of dollars above current levels. The increased costs represent the differential between U.S. and EU pay scales and those found in alternative countries. Costs of separating computer systems would also be driven by the size and complexity of the computer systems. Systems include servers (usually local), applications, databases, and back-up systems. The time needed to implement separation would be significant. If required, we estimate needing twelve (12) months to fully separate computer systems.

For the foregoing reasons, Chemours submits that the proposed definition changes discussed in these comments would cause significant burdens on industry and would change current BIS guidance and policy for computer systems management. Therefore, Chemours urges BIS to consider our suggested change to proposed §734.13(6). Thank you for your consideration of these comments. Please do not hesitate to contact me if you have any questions at 302-773-1318.

Sincerely,

/s/ PEDRO DE LA TORRE

Pedro de la Torre
International Trade Counsel &
Global Compliance Officer
The Chemours Company



*Center for Information on Security Trade Control
4th Floor, Shin-Toranomon Jitsugyo Kaikan,
1-21 Toranomon 1-chome, Minato-Ku, Tokyo 105-0001, Japan
Tel:+81(0)3-3593-1148 <http://www.cistec.or.jp>*

July 31, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division, Office of Exporter Services
Bureau of Industry and Security
US Department of Commerce

Re: RIN0694-AG32 (Proposed rule titled "Revisions to Definitions in the Export Administration Regulations" in 80 FR 31505 dated June 3, 2015)

Dear Ms. Hess:

Thank you so much for your continued supports to us, Center for Information on Security Trade Control (CISTEC), and Japanese industries.

We would refer to your 80 FR 31505 dated June 3, 2015 in which you requested comments on the revisions to definitions in the EAR. We understand through the document that these revisions are based upon the Export Control Reform Initiative, especially the policy of the harmonization of EAR and ITAR. We appreciate these BIS's review and efforts and most of the proposed revisions basically enhance or clarify the current definitions and rules. However, we have concerns on some proposed ones and thus we are pleased to submit to you our comments as stated below.

Also, taking this opportunity, we would like to re-make our ultimate requests on the US reexport control, which we have been making for a very long time.

1. Our comments on the BIS's proposed rules

1. 1. Deemed Reexport Control

(1)Ultimate Request

Please see Section 2.2 below.

(2)Requests until our ultimate request in Section 2.2 is met

The proposed rule §734.20 (a) is based upon the guidance rule quoted below in the

“Deemed Reexport Guidance” dated October 31, 2013 published on the following BIS website. However, the exemption 2.i below of this guidance, which makes it clear there would be no deemed reexport when the foreign national's most recent country of the permanent residency is the same as the country where the release is conducted, is deleted from the proposed rule §734.20(a)(2). We would like to ask BIS to add this exemption 2.i to the proposed rule §734.20(a)(2).

QUOTE (“Deemed Reexport Guidance” of October 31, 2013) (underline added)

A. Legacy BIS Dual and Third Country National Reexport Guidance

In general, you (e.g., an entity outside the United States) may reexport technology or source code subject to the EAR outside the United States to a dual or third country national without an additional license issued by BIS or the application of an EAR license exception if:

1. You are authorized to receive the technology or source code at issue, whether by an individual license, license exception, or situations where no license is required under the EAR for such technology or source code; and
2. You are certain that the foreign national's most recent country of citizenship or permanent residency is either:
 - i. the same as yours (e.g., the same country in which your company outside the United States is located), or
 - ii. that of a country to which export from the United States of the technology or source code at issue would be authorized by the EAR either under a license exception, or in situations where no license under the EAR would be required.

UNQUOTE

<http://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-reexport-guidance>

[Reasons]:

We think it indispensable to make it clear deemed reexport control does not apply to foreign nationals lawfully admitted for permanent residency by adding the above-quoted 2.i to the proposed rule § 734.20(a)(2) because such exemption provided in the current § 734.2(b)(5) quoted below is deleted from the definition of deemed reexport in the proposed rule § 734.14(a)(2) and (b).

QUOTE (Extract of § 734.2(b)(5) of the current EAR)

However, this deemed reexport definition does not apply to persons lawfully admitted

for permanent residence.

UNQUOTE

1.2. New stipulation of the condition “unclassified”

We would like to ask BIS to clearly stipulate the definition of “unclassified” used in the proposed rules §734.7(a) and §734.18(a)(4), as ITAR.

[Reasons] :

Under the proposed rule §734.7(a), one of the conditions of the published technology/software not subject to the EAR is “unclassified”. Under the proposed rule §734.18(a)(4)(i) also stipulates “unclassified” as one of the conditions that sending, taking or storing technology/software is not exports/reexports/transfers. Therefore, without the clear definition of “Unclassified”, there would be confusion of the interpretation and practices of these rules.

1.3. Proposed rule §740.9(a)(3)(License Exception TMP on technologies)

This proposed rule stipulates the license exception TMP on only exports of technologies by or to a US person and a foreign national employee of a US person under certain conditions and thus we would like to ask BIS to add the TMP on reexports of technologies, including those by a non-US person, and the TMP on exports of technologies by a non-US person under substantially the same conditions.

[Reasons] :

We believe the above-requested additions would be appropriate from the viewpoints of fairness between a US person and a non-US person and that between exporters and reexporters.

1.4. BIS Proposal of the deletion of Supplement No.1 to Part734 (Questions and Answers-Technology and Software subject to the EAR)

We would like to ask BIS not to delete this current Supp. No.1 to Part 734 and, as for the questions and answers which should be revised under the new final rules, we would like to ask BIS to do so in the EAR.

[Reasons] :

In this Supp. No.1 to Part734, there are many helpful questions and answers, without which it would be very difficult to precisely interpret the rules stipulated in

Part 734. There would be no guarantee of publishing and keeping these as the guidance on BIS's website if these would be deleted from the EAR. There are some cases where the useful guidelines/criteria in the EAR were deleted from the EAR but they were not published on the BIS website in the past.

1.5. Effective date of the final rules

We would like to ask BIS to make the effective date at least 3 months after the publication of the final rules.

[Reasons] :

The definitions of many kinds of important words and conditions, which are the key bases of the EAR's rules and restrictions, will be revised and thus only one month delay proposed by BIS would not be sufficient, especially for non-US companies, the mother tongue of most of which are not English and, needless to say, the EAR is not their own countries' regulations. The burdens for exactly understanding and preparing for the compliance with this proposed revision of the definitions would be substantially the same as those in case of the recent revisions of the EAR adopting 600 series ECCN, the effective date of which was 6 month delay after the publication of the final rules.

1.6. Rules on reexport cases where US origin chemical materials are incorporated into non-US origin materials and thereby they are substantially transformed

(Note): This request is the follow up of Q & A of the lecture by Mr. Kevin Wolf, Assistant Secretary, BIS, in the US export control seminar in Japan on February 19, 2015, which was held by CISTEC.

Under §560.205(b)(1) of IRANIAN TRANSACTIONS AND SANCTIONS REGULATIONS (ITSR) by OFAC on the following website, the ITSR's restrictions would not apply to the above-captioned reexport cases.

http://www.ecfr.gov/cgi-bin/text-idx?SID=189dfadea50dff52dbee0e8c86bdb996&mc=true&node=se31.3.560_1205&rgn=div8

We would like to ask BIS to stipulate the same kind of the rule on the above-captioned reexport cases also in the EAR or BIS's guidance on the BIS website.

If this stipulation would be difficult, we would like to ask BIS to stipulate de minimis rule (EAR§734.4) can apply also to the above-captioned reexport cases in the EAR or BIS's guidance on the BIS website.

[Reasons] :

There are no clear written rules on the above-captioned reexport cases in the EAR and thus these should be clarified.

2. Our ultimate request

2.1 General

Taking this opportunity, we would like to remind you that it is our ultimate request that the BIS exempt countries including Japan that are members of the international export control treaties/regimes and are implementing robust controls consistent with international standards and norms from re-export controls. We have been requesting this repeatedly in the past as stated in (1) to (5) below. We know that you responded to our request at each time, but would be pleased if you could again consider our request, which is quite reasonable, we believe.

- (1) CISTEC's letter to Mr. Hirschhorn, Under Secretary for Industry and Security, and Mr. Wolf, Assistant Secretary for Export Administration, dated June 29, 2015
- (2) CISTEC's letter to Mr. Mancuso, Under Secretary for Industry and Security, US Department of Commerce, at that time, dated November 7, 2007
- (3) CISTEC's letter to Mr. Wall, Assistant Secretary of Export Administration, BIS, US Department of Commerce, at that time, dated February 19, 2009
- (4) Our oral request to Mr. Wolf when our delegation team visited BIS in Nov. 2011
- (5) Section VI of "RECOMMENDATIONS BY THE GOVERNMENT OF JAPAN TO THE GOVERNMENT OF THE UNITED STATES REGARDING REGULATORY REFORM AND COMPETITION POLICY" dated October 15, 2008
<http://www.mofa.go.jp/region/n-america/us/economy/report0810.pdf>

2.2 Our ultimate and specific request for exemption of deemed reexport control

Especially, we would like to ask BIS to exempt the releases to any of foreign nationals within at least each of "countries including Japan that are members of the international export control treaties/regimes and are implementing robust controls consistent with international standards and norms" from deemed reexport control.

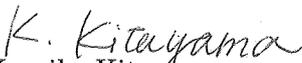
[Reasons]:

In order for non-US companies to comply with the EAR deemed reexport control in their own countries, it is indispensable to confirm the nationality of foreign national employees who may access technologies/sourcecode subject to the EAR and treat each of

them per his/her nationality quite differently. Therefore, there is a serious possibility that the compliance with the deemed reexport control in non-US countries would cause the violation of anti-discrimination laws or privacy laws of their own country. For examples, according to export control attorneys, those laws of EU countries are strictest and thus there are high risks of the violation by the compliance with deemed reexport control in EU countries. Only the proposed rule §734.20(Activities that are not "deemed reexports") would not resolve such risks of the violation.

Once again, we would like to thank you for your assistance and cooperation.

Sincerely,


Kumiko Kitayama

Leader, US Export Control Working Group
Chief, Foreign Regulations Subcommittee
International Research and Relations Committee
Center for Information
on Security Trade Control (CISTEC)



THE UNIVERSITY OF CHICAGO

July 31, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
Washington, DC 20230

RE: RIN 0694-AG32

Dear Sir/Madame:

The University of Chicago ("UChicago") is an Illinois not-for-profit organization that does not accept restrictions on access, publication, dissemination, or participation in research and classroom activities because of one's national origin.

UChicago appreciates the opportunity to comment and respond to the Bureau of Industry and Security ("BIS") RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*. UChicago, additionally, recognizes and appreciates the efforts that the Departments of State, Commerce, and Defense have put into clarifying and harmonizing the pertinent definitions. However, UChicago believes that several of the proposed changes would negatively impact institutions of higher learning; therefore, we offer the following comments:

Changes to Educational Information

Under the proposed rule, some information taught in university courses would not be defined as "educational information" and therefore would become subject to the EAR despite the preamble stating that the "proposed rule is not intended to change the scope of current §734.9."

Existing EAR §734.3(b)(3)(iii) and §734.9 define "educational information" as information "...released by instruction in catalog courses and associated teaching laboratories of academic institutions." Such information is not subject to the scope of the EAR. Despite stating the contrary, the proposed changes remove the existing definition of "educational information" and §734.9 entirely. In lieu, the proposed rule states that "information and software that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution."

Although the proposed rule specifically states that scope of the current §734.9 will not change, UChicago believes that by the very nature of the proposed language, the definition of “educational information” will change. The scope of “educational information” will be far narrower than under the current rule because proposed rule adds the caveat that only “general principles” that are “commonly taught” in schools are exempt from the EAR.

Institutions of higher learning serve the precise purpose of affording its constituents specialized skills and knowledge. Many of the subject matters and areas of concentration, that are usually taught in institutions of higher learning, go beyond what the average person may define as “general principals” that are “commonly taught” in schools. The proposed rule would potentially exclude these types of information and material from its definition of “educational information,” despite the fact that these types of information and material are currently within the scope of “educational information.”

Additionally, as scientific, mathematical, and engineering principles evolve, as do the courses and material that accompany the instruction of those areas. Such new courses and material would not fall within the scope of the proposed definition of “educational information.” Excluding these courses and materials from the definition of “educational information” would discourage growth in these areas.

UChicago believes that such language, “general principles” and “commonly taught,” are ambiguous, at best, and recommends not including “concern general scientific, mathematical, or engineering principles commonly taught in schools” in the proposed rule. Excluding this language would ensure that the definition of “educational information” remain the same as under the current EAR §734.9, as the proposed rule states that it intends to do.

Changes to Fundamental Research

Under the proposed rule, “technology” and “software that rises during or results from fundamental research and “is intended to be published” would be treated differently than under the current EAR.

Existing EAR§734.8(b) states that “publicly available technology and software... [that] arise during, or result from, fundamental research” are not subject to the scope of the EAR. Under the proposed changes, §734.3(a) states that “technology,” which arises during, or results from, fundamental research and “is intended to be published” will not be subject to the scope of the EAR. Further, §734.8(a) goes on to state that “software and commodities are not ‘technology’” resulting from fundamental research.

UChicago believes that the proposed changes would significantly restrict university research. For instance, if “software” and “technology” are results of university research and are published, a natural language document written as a result of the research would be “technology.” However, a computer language document written as a result of the same research would not be “technology” and therefore subject to deemed export restrictions.

UChicago recommends that software arising from fundamental research not be subject to the EAR.

Effective Date of Final Rule

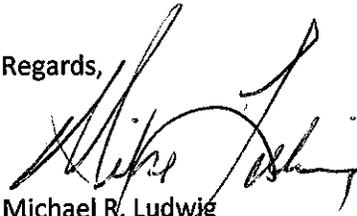
Implementation of RIN0694-AG32 would have a significant regulatory impact on institutions of higher learning, including UChicago. BIS proposes an effective date of 30 days after issuance of the final rule. UChicago believes that due to the significance of these changes, additional time is needed to afford proper implementation. Consequently, UChicago believes a six-month delayed effective date is appropriate.

Other Comments

UChicago works closely with the Council of Governmental Relations ("COGR"), the Association of American Universities ("AAU"), and the Association of University Export Control Officers ("AUECO") and has reviewed their comments being submitted concern the proposed EAR and ITAR changes. Where no UChicago comment is offered, we concur with the comments offered by COGR, AAU, and AUECO.

Again, UChicago appreciates the opportunity to provide these comments to BIS regarding RIN 0694-AG32.

Regards,



Michael R. Ludwig
Assoc. VP for Research Administration & Director, URA

The University of Chicago
University Research Administration
6030 South Ellis Avenue, Room 114 (ED-114)
Chicago, IL 60637
P: 773-702-8604/F: 773-702-2142
E: mrludwig@uchicago.edu

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
US Department of Commerce
14th Street and Pennsylvania Avenue, NW
Washington, DC 20230

(Submitted by e-mail on 3 August 2015 publiccomments@bis.doc.gov)

Subject: Definitions in the Export Administration Regulations RIN:0694-AG32

Dear Sir/Madam:

I appreciate the opportunity to comment on this rule. After careful review I believe that, as written, the language strictly interpreted has a number of potentially draconian unintended consequences. I would respectfully submit that these need to be addressed before the four questions posed under Request for Comments can be reasonably answered.

General Comments:

Until current export control reform process is completed and the aggregate effects of changes to and interactions between the EAR and ITAR are fully understood the practical effects of either are going to be virtually impossible to assess. This is particularly true of definitions addressed in this proposed rule, whose interpretation affects the rest of the regulations.

Some of the items in the CCL tend to be broadly categorical. Thus, their practical effect depends on the definition of terms used, and specifically on the language of notes, exceptions, and references to other provisions in the definitions. In the process, the goal of a “positive list” has been lost. The current list is “positive” only in the sense that the top level paragraphs specifying the scope of controlled items are nominally positive statements.

The proposed language allows for widely divergent interpretations. The flexibility this affords the government may arguably streamline government export administration. But, I would respectfully submit that the resulting language will make it far more difficult (in some cases, virtually impossible) for US companies, academic researchers, and even citizens in their day-to-day lives to determine what constitutes a violation of the regulations.

Exporters and researchers can always ask the government for guidance. However, daily interactions between US and foreign citizens across a wide range of technical subjects through a wide range of communication modes are pervasive. In a free and open society, companies academic researchers and ordinary citizens should not have to ask the government’s

permission to engage in what are otherwise normal and legal day-to-day commercial and scientific activities.

Reliance of the US military on Commercial Off-the-Shelf Technology (COTS) makes it difficult to discern a “bright line” between civil and military technology.

It is a given that the US is part of an international agreement, the Wassenaar Arrangement (WA). While the WA is not a formal treaty organization, the US has both legal and moral responsibilities to conform to its terms and condition.

But, as the saying goes, the devil is in the details. Much of the specific language (particularly in some of the more problematic definitions and notes) does not appear in the Wassenaar. Examples in the EAR are the definitions of “specially designed” and the proposed definition of “peculiarly responsible”). This language is specific to the US. Even when US regulations adopt language verbatim from the WA text, such US-only provisions affect how it is read and enforced.

§ 734.3 Items subject to the EAR.

The effects of this language are heavily modulated by language throughout the proposed rule. The General Comments apply.

§ 734.7 Published.

The provisions of *subparagraph “(4) Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the Internet on sites available to the public; “* entails several definitional difficulties. The strict letter of can be met by posting the data on line for an arbitrarily short period of time. (Duration is not a criterion), posting under URL/domain names that are unrelated to or obscure the nature of the content or posting on a site available to the public, but, in an obscure foreign language or in an encrypted form. (I recognize this is legal hair-splitting—and that this is the kind of challenge the government has faced in creating the proposed language.)

The “i.e., unlimited distribution” creates a very large potential loophole. Specifically, would this catch information made available for download on the condition that the person downloading agree to specific restrictions on further dissemination and use of the data as a condition of the download.

Finally, the language does not appear to address the case of information posted by someone other than the rightful owner. This is a common occurrence on the internet, without restrictions that the owner would have placed on further dissemination and use.

§ 734.8 “Technology” that arises during, or results from, fundamental research.

As a general comment, the language proposed for the EAR appears to avoid some of the serious difficulties of the corresponding language in the ITAR. A minor issue is noted in Note 1 to paragraph (a) which reads as follows:

The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technology that arises during or results from fundamental research” except to the extent that such inputs are “technology” that arose during or resulted from earlier fundamental research.

I would respectfully suggest that any information of practical value in current fundamental research was almost certainly the subject and result of earlier fundamental research at some point in time. Thus the language appears to say that the results of ongoing cutting edge fundamental research are not considered technology subject to the EAR, but that information from prior research may be.

This may reflect the premise that technology that has matured sufficiently to be used as the basis for future research warrants control.

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

* * * * *

Peculiarly responsible.

The definition reads:

An item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR.

The existing definition of “specially designed” in the EAR has been the subject of much discussion and comment because of its breadth, and the circular nature of the definition when applied to an item specifying “specially designed” as an attribute. Specially designed is currently defined as:

“As a result of “development” has properties peculiarly responsible for achieving or exceeding the performance levels, characteristics, or functions in the relevant ECCN or U.S. Munitions List (USML) paragraph”

The presumption is that, at some point, the defined term “peculiarly responsible” will be incorporated. If so, as written, it will compound the problem by equating “peculiarly responsible” with “used in”. This will be a stunning overreach. From participating in discussions on specially designed, I do not believe this is BIS’s intent.

I believe that the intent is a combination of the sense in which Technologies “D” and “E” are deemed “required” in the explanatory note, with an added provision that to be considered peculiarly responsible the item or technology must actually be used in or for production of a controlled item. I would respectfully offer this as a potential way forward.

“Required.”

The definition of “required” is clear, and the reference to the GTN helpful. I would respectfully submit that in the example given, Technologies “D” and “E” are peculiarly responsible for the specified performance. This points the way to a much better solution than the language of the proposed rule for which the criteria for “peculiarly responsible” is effectively “used in. . .” (See comment on “peculiarly responsible”, above.)

A general comment on Note 1 to the Definition of “required” is that the choice of military aircraft as an example obscures potential difficulties in applying the definitions to the more general case of dual-use civil products. In the broader context, because of the large and growing reliance of the military on COTS, the characteristics and features of controlled products are likely to be quintessentially civil in nature, and less clear.

“Technology”

The exceptions set forth in (b) of this definition are very narrow in scope. I believe that the aggregate effect of the language in this proposed rule would be to capture a standard user’s manual for a family of equipment if one of the models exceeded a control parameter on the CCL. (This issue is more problematic for dual-use products, where civil and military variants of products exist. Comments to DDTC on the proposed ITAR rule will address this.)

Commercial practices with regard to this type of technical data vary greatly depending on its perceived value and what the manufacturer’s marketing strategy. Manuals may be made available on line for download without restriction; to registered owners of the product, or for a fee.

This is but one obvious example of a myriad of exchanges and transactions that occur thousands of times on a daily basis that the proposed language can be interpreted as bringing making ordinary exchanges of information export controlled. The implied restrictions on oral communications, if applied strictly, pose a potentially serious threat to basic First Amendment rights.

It is not clear how the implied release in the definition of “published” applies here, since “published does not appear in the exceptions in (b).

Closing Observations

The task the government took on in attempting to reform export controls is daunting in the extreme. Considering the results to date, I would respectfully suggest the expectation of effective reform within a legislative framework that is now half a century old, may have been unreasonable. Many of the fundamental concepts that shaped the process, such as the 1976 DSB study, commonly referred to as “the Bucky Report” and the 2009 National Academy Study, Beyond Fortress America sponsored by the National Academies are no longer current. The flaw these and in export control reform generally was to focus on the perceived flaws in the current system.

My personal belief, after over half a century in national security, is that effective reform cannot occur in isolation from the broader range of national goals and objectives. True reform must begin a better understanding, not just of the historical problems of the existing system, but on the purpose of export controls looking outward and ahead.

Again, I appreciate the work represented in this proposed rule and the opportunity to offer comments.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "A. Ramsbotham, Jr.", with a long horizontal flourish extending to the right.

Alan J. Ramsbotham, Jr.
King George, VA 22485



**The Research
Foundation for**

The State University of New York

Stony Brook University

*Office of the
Vice President of Research*

August 3, 2015

*S5422 Frank Melville Library
Stony Brook, NY 11794*

*Telephone: 631-632-7932
Fax: 631-632-5074*

www.stonybrook.edu/research

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am writing on behalf of State University of New York at Stony Brook ("SBU"), a public academic, research and medical center and member of the American Association of Universities (AAU) and the Council on Governmental Relations (COGR). SBU concurs and supports the joint comment letter submitted by AAU and COGR as well as the comment letter submitted by the Association of University Export Control Officers (AUECO).

SBU appreciates the opportunity to offer further comment on the proposed Revisions to Definitions in the Export Administration Regulations (EAR) and corresponding changes to the International Traffic in Arms Regulations (ITAR) as they will have a significant impact on SBU and other U.S. academic institutions.

SBU primarily conducts fundamental research and educates students of all nationalities. The State University of New York policies require (1) research activities to be open for participation of foreign nationals, (2) conduct, progress and results of sponsored research to be unrestricted for dissemination, and (3) non-discrimination based on citizenship or national origin in all academic programs. We believe that there are additional areas in the proposed revisions to the definitions that require further harmonization or clarification to avoid a negative effect on research and education at SBU and other U.S. academic/research institutions.

Changes to Educational Information

In the proposed rule, the definition of “educational information” is removed, and §734.3(b)(3)(iii) excludes information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution.

The proposed change adds uncertainty and potentially narrows the scope of applicability of the exclusion. For example, will SBU when contemplating new curricular additions need to be concerned that the course may not be commonly taught at other universities? Would the content of catalog courses that include hands on design laboratories, such a capstone experience (multi-faceted assignment that serves as a culminating academic experience for students), previously treated as “educational information” become subject to the EAR by virtue of including more than general principles? A narrow interpretation of the revised §734.3(b)(3)(iii) would inhibit the ability of the SBU to develop new courses in emerging areas in science and engineering critical to employability of their graduates and the future competitiveness of the industrial sector.

SBU prefers that the qualifier “concern general scientific, mathematical, or engineering principles commonly taught in schools” be removed and that the simpler “is released by instruction in catalog courses and associated teaching laboratories of academic institutions “ be retained for §734.3(b)(3)(iii).

As an alternative, changing the proposed description to “information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and /or released by instruction in a catalog course or associated teaching laboratory of an academic institution” would describe educational information more fully without narrowing the scope of the exclusion.

Definition of “Fundamental Research”

SBU supports the proposed definition of “fundamental research” using the language of NSDD-189 in the EAR and the ITAR as it is consistent with our understanding of the concept. SBU also generally supports the alternate definition: “fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community with the assumption that it would not alter the proposed language of permitting prepublication review under specific circumstances within the fundamental research domain.

If the NSDD definition is selected, the proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18) with an alternate definition adopting OMB Circular A-11 language. SBU favors the adoption of the OMB Circular A-11 language as it is already used in the context of reporting federal expenditure to NSF. If the DFARS definition is adopted, the inclusion of the rest of 48 CFR part 31.205-18, “Applied research does not include efforts whose principal aim is design,

development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development, defined in this subsection" would help clarify "applied research". The "for sale" criterion would clearly distinguish "applied research" and "development" activities.

SBU requests that the specific language of §734.8(b) be retained in the EAR or that BIS develop a decision tree tool for the determination of fundamental research for universities that incorporates the current criteria for university based fundamental research. As a primarily fundamental research institution, SBU uses §734.8(b) to make determinations as to the applicability of fundamental research by evaluating proposed research activities using paragraphs 2 -6, and assuming that the research qualifies as "fundamental research" if all conditions are met.

"Fundamental research", "technology", and "software"

Currently, SBU fundamental research includes the creation of software as a research result and/or a research tool. For example, SBU is the recipient of federal grants where the research result is software that is intended to be shared broadly. In fact, in some cases it is a requirement of the grant to share the resulting software with the larger academic community.

The proposed change under §734.8(a) would significantly complicate and restrict university research; while natural-language documents written by a researcher would be "technology" that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions.

Under the proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is "intended to be published" would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. The proposed rule refers to a proposed note "to clarify that software and commodities are not 'technology resulting from fundamental research'" (although we were unable to locate the note). Software resulting from university research is "published" as well as "technology", as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology.

SBU supports AUECO's recommendation that §734.8(a) be revised as follows:

§ 734.8 "Technology" and "software" that arises during, or results from, fundamental research.

(a) "Technology" or "software" that arises during, or results from, fundamental research and is 'intended to be published' is not "subject to the EAR."

(b) Prepublication review. "Technology" or "software" that arises during, or results, from fundamental research is "intended to be published" to the extent that the researchers are free to publish the technology and software source code without restriction or delay. "Technology" that arises during or

results from fundamental research subject to prepublication review is still "intended to be published" when:

Questions and Answers- Technology and Software Subject to the EAR

SBU is concerned that the removal of the questions and answers found in Supplement No. 1 to part 734 in the regulations, which we use to guide export control decisions, would create an increased uncertainty in our applications of key concepts including fundamental research, publication, and educational instruction. While SBU agrees and recognizes that the questions and answers are illustrative, we encourage that BIS retain them.

End to End Encryption Standard

The addition of §734.18 listing activities that are not exports, reexports or transfers is a useful addition to the EAR. In particular, the exclusion of sending, taking or storing software that is secured using end-to-end encryption from export activities is welcome to the academic research community as it will reduce the faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. SBU favors the proposed EAR illustrative standard of FIPS 140-2 supplemented in accordance with NIST guidance or other similarly effective means.

Effective Date of the Final Rule

Although the revised definitions do not make changes to the USML or the CCL, as written they have a significant impact on regulatory burden for U.S. universities. If the proposed changes to ITAR §120.49(b) Prepublication Review go to final rule without changes, SBU will need to significantly change their business practices associated with review and negotiation of sponsored research agreements as well as the management of access to sponsored research.

SBU, like most other institutions, seeks a balance when negotiating contracts with industry for university research. Most industry sponsors, as well as many foundations, acknowledge the institution's right to publish the results of the research but also require limited time prepublication review to prevent the inadvertent disclosure of sponsor proprietary information and to permit seeking of patent protection as applicable. SBU, along with other U.S. universities, has until now interpreted such reviews as within the scope of fundamental research.

Further these changes will require implementation of new procedures to determine applicability of the ITAR to fundamental research with prepublication review, implementation of technology control plans and submission of license applications for the participation of foreign nationals in the research, monitoring of those plans, and eventual removal of the plans once the prepublication review has occurred, as well as revised export compliance training for affected departments on campus. More importantly, such review would be required retrospectively for current projects. These procedures will also require additional staffing for export compliance. Universities will not be able to meet the compliance obligations imposed by the addition of the prepublication review language of ITAR §120.49(b) within 30 days of

the publication date. SBU suggests at minimum a 6-month delay in effective date, and further that the revised regulations be applicable only to new sponsored research begun after the effective date of the Final Rule.

SBU appreciates the opportunity to provide comments on these proposed changes.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "David Conover", written over the typed name.

David Conover

Vice President for Research,
Operations Manager,
The Research Foundation for SUNY



LORD Corporation
World Headquarters
111 Lord Drive
Cary, NC 27511-7923
USA

July 31, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

Email: publiccomments@bis.doc.gov

RE: RIN 0694-AG32

LORD Corporation (“LORD”) appreciates the opportunity to review and comment on the proposed rule to harmonize and clarify many of the definitions between the Export Administration Regulations (“EAR”) and the International Traffic in Arms Regulations (“ITAR”) as part of the ongoing Export Control Reform Initiative.

Our comments and concerns, along with suggested recommendations are as follows:

1. §772.1 – Definitions. “Required” and “Peculiarly Responsible”

- The effort to include and define ‘peculiarly responsible’ as part of the harmonization of definitions is appreciated, as we have become accustomed to relating and applying this verbiage when determining if an item is “specially designed”. The determination is based upon there being an item that results from development, which has some properties that are unique or peculiarly responsible that enable it to achieve or exceed controlled performance levels, functions or characteristics described in a relevant ECCN or USML paragraph. However, we find it challenging to apply the same process methodology to technical data as proposed in the definitions for “required” and “peculiarly responsible”.
- The insertion of the term “peculiarly responsible” into the first sentence of the “required” definition does not add value or provide clarification.
- The example provided after the statement ‘*Such “required” “technology” or “software” may be shared by different products*’, does not seem to be representative of how required technology may be shared, but rather appears to make distinctions between technologies which are “required” and not “required”. If this is correct, it is suggested that the statement ‘*Such “required” “technology” or “software” may be shared by different products*’, be placed elsewhere to avoid confusion.

- The proposed language for defining “peculiarly responsible” seems to be intended to parallel the language contained in “specially designed” as defined in EAR §772.1. However, as currently written, it lacks any parameters or reference points such as ‘item’, ‘development’, and ‘properties’.
- The proposed definition of “peculiarly responsible” appears to be directed at an item, however, the language of subparagraph (3) uses the term ‘information’ which we assimilate to technology or technical data.
- In subparagraph (3), the word ‘identical’ is used as opposed to language that is more aligned with the phrase ‘same or equivalent’ as used in the definition for “specially designed”.

Recommendations:

Following are recommended changes for consideration to the language proposed in §772.1:

“Required”

*As applied to technical data, the term ‘required’ refers to only that portion of technical data that is **necessary** ~~peculiarly responsible~~ for achieving or exceeding the controlled performance levels, characteristics or functions of a relevant ECCN or U.S.. Munitions List paragraph unless:*

- 1. The Department of Commerce has determined otherwise in a commodity classification determination;*
- 2. Reserved;*
- 3. It is technically and functionally equivalent to information used in or with a commodity or software that:*
 - (i) Is or was in production (i.e., not in development); and*
 - (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;*
- 4. It was or is being developed with “knowledge” that it is or would be for use in or with commodities or software (i) described in an ECCN and (ii) also commodities or software either not ‘enumerated’ on the CCL or USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;*
- 5. It was or is being developed for use in or with general purpose commodities or software (i.e., with no knowledge that it would be for use in or with a particular commodity or type of commodity); or*
- 6. It was or is being developed with “knowledge” that it would be for use in or with commodities or software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) exclusively for use in or with EAR99 commodities or software.*

For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Such required technical data may be shared by different products.

[continue with the language as written in Notes 1 and 2]

~~“Peculiarly responsible”~~—[Delete this definition]

2. §734.13 Export

The proposed changes to the definition of ‘export’ are an improvement from the current language. In an attempt to better parallel the EAR definition of “export” with the ITAR definition provided in §120.17, it is recommended that language be added to acknowledge the fact that the EAR has no equivalent to the ITAR ‘defense services’. The addition of such language is in line with this harmonization effort, and would serve as written confirmation that ‘defense services’ are specific to only the ITAR.

3. §734.18 Activities that are not exports, reexports, or transfers

The addition of this section is a welcomed update and in particular, the inclusion of subparagraph (a)(4) that speaks to sending, taking, or storing “technology” and “software” as well as the supplemental information provided in subparagraphs (b) and (c). The proposed language of (a)(4) and (b) are the particular sections for which we have some concerns.

- ‘End-to-end encryption’ may be interpreted as more stringent, and in some cases, less stringent than FIPS 140-2, and could be a stand-alone requirement, independent of (iii). For example, if a sufficient ‘end-to-end encryption’ scheme is employed to protect a given data set, then the additional requirement of a FIPS 140-2 Level 3 certified product to transmit via TLS, such as an IPsec VPN, is redundant. The concern revolves around the differences between ‘end-to-end encryption’ and FIPS 140-2. To remove ambiguity, clarification on what parameters constitute sufficient ‘end-to-end encryption’ and when ‘end-to-end encryption’ versus a validated FIPS 140-1/FIPS 140-2 cryptographic module is required, is needed.
- The definition provided for ‘end-to-end encryption’ speaks to an originator and an intended recipient, but does not clarify whether an originator means one individual person or one company/entity. In the case of utilizing cloud storage, it would not be unreasonable for companies to need ‘many to one’ encryption. If the intention of ‘originator’ is one individual person, companies could incur increased burden and costs by having to obtain individual certificate keys for each employee.

Recommendations:

- Clarification on what parameters constitute sufficient ‘end-to-end encryption’,’
- Clarification on when ‘end-to-end encryption’ versus a validated FIPS 140-1/FIPS 140-2 cryptographic module is required, is needed (based on recommendation below)
- It is suggested that the language set forth in (a)(4) be considered as follows as well as including a note that provides clarity to the requirements:

(a)(4) *Sending, taking or storing “technology” or “software” that is:*

- (i) *Unclassified;*
- ~~(ii)(iv)~~ *Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation;*
- (iii) *Secured using cryptographic modules (hardware or “software”) compliance with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and*
- ~~(iv)(ii)~~ *Secured using ‘end-to-end encryption’.*

Note to (a)(4): Technology secured using the end-to-end encryption method described in (iv), does not require the additional encryption method described in (iii). However, if technology is secured using the method described in (iii), then the end-to-end encryption method described in (iv) must also be in place.

- (b) *Definitions. For purposes of this section, ‘end-to-end encryption’ means the provision of uninterrupted cryptographic protection of data between ~~an~~ **one originating party (one individual or entity)** and ~~an~~ **one** intended recipient, including between one ~~an~~ individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.*

4. §740.9(a)(3)

We are seeking clarification as to whether the exception cited in §740.9(a)(3) may be used to authorize the remote access by a U.S. person or foreign person employee of a U.S. company to technical data maintained on a company server that is located in the United States while they are outside of the United States.

Additional facts:

- 1) U.S. person or foreign person employee is on travel or temporary assignment outside of the United States;
- 2) Foreign person employee is authorized to receive the technical data;
- 3) Access is achieved using a secure/encrypted connection; and
- 4) The server in which the technical data is stored is secure/encrypted.

If this exemption is permitted to be used to access technical data as described above, it would be helpful to include 'access' in this section.

Once again, we appreciate the opportunity to provide comments on these proposed changes. If you have questions or need additional information, please do not hesitate to contact me at 919-342-2378 or at marjorie.alquist@lord.com.

Sincerely yours,

A handwritten signature in blue ink, appearing to read "Marjorie L. Alquist". The signature is fluid and cursive, with a large initial "M" and a long, sweeping tail.

Marjorie L. Alquist
Manager, Global Trade Compliance



July 28, 2015

Sent via email to: publiccomments@bis.doc.gov and DDTCTPublicComments@state.gov

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue NW
Washington, DC 20230

and

Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
Bureau of Political Military Affairs
Department of State
Washington, DC 20522

Subjects: RIN 0694-AG32 - Revisions to Definitions in the Export Administration Regulations

and RIN 1400-AD70 International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions

Dear Sir or Madam:

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry. With approximately 2,000 member companies, 3,000 academic and training partners and nearly 2 million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

Thank you for the opportunity to provide comments on these proposed rules which are part of the Administration's Export Control Reform Initiative. RIN 0694-AG32 proposes revisions to the Export Administration Regulations (EAR) to include the definitions of "technology," "required," "peculiarly responsible," "proscribed person," "published," results of "fundamental

research," "export," "reexport," "release," "transfer," and "transfer (in-country)" to enhance clarity and consistency with terms also found on the International Traffic in Arms Regulations (ITAR). The rule also proposes amendments to the Scope part of the EAR to update and clarify application of controls to electronically transmitted and stored technology and software.

RIN 1400-AD70 proposes to amend the ITAR to update the definitions of "defense article," "defense services," "technical data," "public domain," "export," and "reexport or retransfer" in order to clarify the scope of activities and information that are covered within these definitions and harmonize the definitions with the EAR, to the extent appropriate. Additionally, the Department of State proposes to create definitions of "required," "technical data that arises during, or results from, fundamental research," "release," "retransfer," and "activities that are not exports, reexports, or retransfers" in order to clarify and support the interpretation of the revised definitions that are proposed in this rulemaking. The Department proposes to create new sections detailing the scope of licenses, unauthorized releases of information, and the "release" of secured information, and revises the sections on "exports" of "technical data" to U.S. persons abroad. Finally, the Department proposes to address the electronic transmission and storage of unclassified "technical data" via foreign communications infrastructure. This rulemaking proposes that the electronic transmission of unclassified "technical data" abroad is not an "export," provided that the data is sufficiently secured to prevent access by foreign persons. Additionally, this proposed rule would allow for the electronic storage of unclassified "technical data" abroad, provided that the data is secured to prevent access by parties unauthorized to access such data.

CompTIA has the following comments on the proposed rules.

Definition of Technology

Proposed Section 772.1(a)(1) defines "Technology" as:

"Information *necessary* for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control "technology")...." (Emphasis added.)

The definition in Section 772.1(a)(1) should be made consistent with the General Technology Note and the proposed definition of technical data in Section 120.10(a)(1) of the ITAR. Specifically, in the definition the word "necessary" should be replaced with the word "required."

In addition, the references to "operation, installation, maintenance, repair, overhaul, or refurbishing" also should be deleted from the definition. While CompTIA members understand that these items are likely referenced as a result of certain "600 series" technologies, the inclusion of these items individually in the proposed definition is unnecessary and creates confusion. Among other things, the use of the separate terms, which are encompassed in the definition of "use," create a circular reference to the definition of "use" in the EAR. In addition,

the separate terms may have the unintended consequence of making items such as unpublished user manuals that do not meet the definition of “use” subject to the EAR (albeit classified as EAR99) when such manuals were not previously subject to the regulations. CompTIA believes that such confusion can be eliminated by revising the proposed definition to eliminate the specific reference to these terms and instead state: “Information [required] for the “development,” “production,” “use,” or other terms specified in ECCNs on the CCL that control “technology”....”

Proposed Section 772.1(a)(5) and proposed Section 120.10(a)(5) also define “technology” and “technical data,” respectively, to include information such as decryption keys, network access codes or passwords that allow access to other “technology” in clear text or software. These proposed definitions could be read to include as “technology” and “technical data” certain hardware or software – such as key fobs, tokens and even VPN software – that are used to access technical information. Additional clarification is required regarding these definitions so as to avoid confusion in determining whether an item is hardware, software or technology.

Finally, proposed Section 772.1(b)(1) and proposed Section 120.10(b)(1) state that “technology” and “technical data,” respectively, do not include “non-proprietary general system descriptions.” It is not clear what is intended by the use of the term “non-proprietary” in these proposed definitions. Specifically, it is not clear whether the intent of the definition is to exclude general systems descriptions only if they are published or in the public domain, respectively. The ITAR currently excludes from the definition of technical data “general systems descriptions” as well as (*i.e.*, in addition to) information in the public domain. Moreover, a system description may be general (*i.e.*, not reveal technical details about an item) but still “proprietary” such as descriptions regarding a system included in specific, unpublished proposals in response to RFPs. CompTIA therefore suggests that Commerce and State eliminate the reference to “non-proprietary” in proposed Section 772.1(b)(1) and proposed Section 120.10(b)(1).

Definition of Public Domain

CompTIA submits that the proposal to require U.S. Government review before any publication of technical information, as specified in proposed Section 120.11(b), is an unconstitutional restraint of free speech. The ITAR do not currently require U.S. Government review before publication of technical data or software.

Arises During, or Results from, Fundamental Research

Proposed Section 120.49(b) should be revised to be consistent with the language set forth in proposed Section 734.8(b). Section 734.8(b) provides greater clarity regarding when technology would be considered to be “intended to be published.” In addition to providing more thorough guidance to exporters, incorporating the additional details into proposed Section 120.49(b) also would achieve greater consistency between the regulations.

Patents

Proposed Section 734.10

The newly proposed regulation should be revised to read:

“Technology” is not “subject to the EAR” if it is contained in *any of the following*:

- (a) A patent or an open (published) patent application available from or at any patent office;
- (b) A published patent or patent application prepared wholly from foreign-origin technology where the application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office;
- (c) A patent application, or an amendment, modification, supplement or division of an application, and authorized for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office, 37 CFR part 5; or
- (d) A patent application when sent to a foreign country before or within six months after the filing of a United States patent application for the purpose of obtaining the signature of an inventor who was in the United States when the invention was made or who is a co-inventor with a person residing in the United States.

Development

§120.47

The newly proposed regulation should be revised to read:

Development is related to all stages prior to serial production, such as, *but not limited to*: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. Development includes modification of the design of an existing item.

Required & Peculiarly responsible (in the EAR)

CompTIA recommends that “identical” be replaced by “substantially similar” in Section 772.1(3).

§772.1 “Required”. (General Technology Note)—

As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such “required” “technology” or “software” may be shared by different products. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Note 1: The references to “characteristics” and “functions” are not limited to entries on the CCL that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, ECCN 9A610.a controls “military aircraft specially designed for a military use that are not enumerated in USML paragraph VIII(a).” No performance level is identified in the entry, but the control characteristic of the aircraft is that it is specially designed “for military use.” Thus, any technology, regardless of significance, peculiar to making an aircraft “for military use” as opposed to, for example, an aircraft controlled under ECCN 9A991.a, would be technical data “required” for an aircraft specially designed for military use thus controlled under ECCN 9E610.

Note 2: The ITAR and the EAR often divide within each set of regulations or between each set of regulations (a) controls on parts, components, accessories, attachments, and software and

(b) controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated. Moreover, with the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data or “technology” is the same as the jurisdictional status of the defense article or “item subject to the EAR” to which it is directly related. Thus, if technology is directly related to the production of a 9A610.x aircraft component that is to be integrated or installed in a USML VIII(a) aircraft, then the technology is controlled under ECCN 9E610, not USML VIII(i).

772.1 *Peculiarly responsible.* An item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation,

maintenance, repair, overhaul, or refurbishing of an item subject to the EAR unless:

(1) The Department of Commerce has determined otherwise in a commodity classification determination;

(2) Reserved;

(3) It is **substantially similar** to information used in or with a commodity or software that:

(i) Is or was in production (*i.e.*, not in development); and

(ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(4) It was or is being developed with “knowledge” that it would be for use in or with commodities or software (i) described in an ECCN *and* (ii) also commodities or software either not ‘enumerated’ on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;

(5) It was or is being developed for use in or with general purpose commodities or software, *i.e.*, with no “knowledge” that it would be for use in or with a particular commodity or type of commodity; *or*

(6) It was or is being developed with “knowledge” that it would be for use in or with commodities or software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) exclusively for use in or with EAR99 commodities or software.

Definition of "Export"

1. BIS should delete the term "or permit" from proposed Section 734.13(a)(6).

This section defines as an export:

“Releasing or transferring decryption keys, network access codes, passwords, software, or other data with “knowledge” that such provision will cause **or permit** the transfer of other technology or software in clear text to a foreign national.”

Liability for exporters should only be created when "knowledge" of an actual transfer of controlled material takes place. The phrase "or permit" would create liability for mere theoretical access. By their very nature, decryption keys, network access codes, passwords, etc. permit access to the related protected material. Thus, to some extent, any transfer of decryption keys, network access codes, passwords necessarily would result in knowing that access to the protected materials has been permitted. Accordingly, BIS should delete the term "or permit" from proposed Section 734.13(a)(6).

2. BIS should add the modified "knowledge" provisions of Section 734.13(a)(6) to the deemed export rule in proposed Section 734.13(a)(2).

Proposed Section 734.13(a)(2) defines as a deemed export:

"Releasing or otherwise transferring "technology" or "source code" (but not "object code") to a foreign national in the United States (a "deemed export")."

The definition of "technology" in Proposed Section 772.1(a)(5) includes "Information, such as decryption keys, network access codes, or passwords that would allow access to other "technology" in clear text or "software.'" Therefore, any transfer of a decryption key, etc. to a foreign national in the United States would be treated as a deemed export.

Section 734.13(a)(2) should be made consistent with (a)(6) and include an equivalent "knowledge" requirement. The rationale for including a "knowledge" requirement in (a)(6) -- and limiting it to "knowledge" of actual, not theoretical, access to controlled materials is identical to requiring "knowledge" of actual, not theoretical, access to controlled "technology" or "source code" for purposes of a deemed export.

Accordingly, Section 734.13(a)(2) should be changed to read:

"Releasing or otherwise transferring "technology" or "source code" (but not "object code") to a foreign national in the United States (a "deemed export"). Releasing or transferring decryption keys, network access codes, passwords, software, or other data is a deemed export when done with "knowledge" that such provision will cause the transfer of other technology or software in clear text to a foreign national."

Definition of Reexport & Deemed Reexport

The comments and recommendations above regarding "export," "deemed export," and "or permit" also apply to "reexport" and "deemed reexport."

Activities That Are Not Exports, Reexports, Releases, Retransfers, or Transfers

Proposed Section 734.18(a) lists a number of activities that are not treated as exports, reexports, or transfers for purposes of the EAR. Section 734.18(a)(4) includes sending, taking, or storing "technology" or "software" that is, among other things, secured using 'end-to-end encryption.' Section 734.18(b) states that "'end-to-end encryption' means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the

data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider."

Although the creation of this exclusion from the scope of the EAR is useful, it is unlikely to be used widely. End-to-end encryption is very uncommon in cloud computing environments. Where it exists, it is used most frequently in cloud storage services. However, it does not even represent the majority of usage in cloud storage environments. Outside of cloud storage, end-to-end encryption is used even more rarely in the provision of cloud-based services. Introducing end-to-end encryption to cloud services results in the loss of too many useful features that cloud computing customers want offered to them. Accordingly, the overwhelming majority of cloud computing providers, users, and uses will fall outside the scope of proposed Section 734.18. The proposed regulation does not make clear how it intends to treat cloud transactions in environments that don't use end-to-end encryption. Based on conversations with BIS, our understanding is that those transactions would be governed by the existing advisory opinions that BIS has issued on cloud computing, which industry has relied upon for the last several years.

Release of Protected Information

Proposed Section 127.1(b)(4) should be revised to require that for a violation to occur the release or transfer of information must be made with "knowledge" that such a release will result, directly or indirectly, in an unauthorized export, reexport, or retransfer. Such a requirement would be consistent with the knowledge element set forth in the corresponding violations provision in proposed Section 764.2(l). In addition, it would ensure that persons are not prosecuted for situations in which they would not have any actual knowledge or reason to know that the release of a password would result in an unauthorized export, reexport or retransfer of technical data.

Proposed Section 127.1(a)(6) Prohibition

The newly proposed prohibition set forth in Section 127.1(a)(6) should be revised to clarify that it is a violation of the ITAR to export, reexport, retransfer or otherwise make available to the public technical data or software if a person has actual knowledge that the items were made available without U.S. Government review. Today, many companies incorporate and republish information available on the internet. It is not feasible for an exporter to discern whether that information was previously released with authorization – much less who was the original party that released the information. At minimum, this provision should be clarified to exempt from prosecution companies that, without actual knowledge, republish information that was previously released on the Internet or in other settings.

Thank you once again for the opportunity to provide comments on the proposed rules.

Sincerely,

A handwritten signature in black ink, appearing to read "Ken Montgomery". The signature is written in a cursive style with a large, looping initial "K".

Ken Montgomery

Vice President, International Trade Regulation & Compliance

August 3, 2015

Hillary Hess, Director
Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Avenue, NW
Washington, DC 20230

Re: Proposed Revisions to Definitions in the Export Administration Regulations
RIN 0694-AG32

Dear Bureau of Industry and Security,

Thank you for inviting comments on the proposed changes to the Export Administration Regulations (RIN 0694-AG32). We welcome this opportunity to address the impacts envisioned by the proposed rule on Duke University and similar academic research institutions.

Comments related to specific proposed changes:

734.8 “Technology that arises during, or results from, fundamental research:

Paragraph (a) removes “software” from the definition of fundamental research. We request that BIS include both technology and software since software resulting from a university research project may also be published. Indeed, proposed 734.3(b) already identifies “information and “software”” as items that are not subject to the EAR.

The existing language in 734.8(b) states that, “Research conducted by scientists, engineers, or students at a university normally will be considered fundamental research, as described in paragraphs (b)(2) through (6) of this section.” This presumption has been removed in proposed 734.8. We urge BIS to restate the current language in the final rule.

Paragraph (c) includes a proposed definition of “fundamental research”. We prefer the language proposed in paragraph (c) over the alternate definition which is slightly confusing since patents are occasionally sought for the products of fundamental research. We believe that the term “non-proprietary research” may be confusing to the academic community. The proposed definition which more closely follows NSDD-189 has been used by a number of government administrations and has been widely accepted by the research community.

We support inclusion of definitions for “basic research” and “applied research” since this issue is often a stumbling block during negotiation of research contracts with US government agencies. Inclusion of the definitions in the regulations will discourage government contracting officers from defaulting to a stance that their research is one of the exceptions to NSDD-189.

734.11 Government-sponsored research covered by contract controls:

The language, based upon existing 734.11(a), has been a source of confusion for universities. We prefer that the ITAR language proposed in 120.49(b) Note 3 be used instead.

In addition, we find that the examples in existing 734.11(b) are helpful and should be retained.

734.13 Export

Paragraph (a) appears to have a typographical error, referring to 734.17, instead of 734.18.

We prefer the proposed EAR definition in 734.13(a)(6), which requires “knowledge” that releasing decryption keys, etc. will result in the release of controlled technology as opposed to the proposed ITAR definition [22 CFR §120.17(a)(6)], which would consider it an export “regardless of whether such data has been or will be transferred,” since no there obviously cannot be an export if no data is ever provided. However, paragraph 734.13(a)(6) is cumbersome and could lead to confusion. In order to clarify, we suggest replacing the second “other” in the paragraph with “controlled.”

We request that BIS clarify the language proposed in § 734.13(b) in stating that an export occurring in the United States is considered an export to the foreign national’s most recent country of citizenship or permanent residence. Is there a hierarchy in determining whether citizenship or permanent residency should be used? Should the export be considered deemed to both countries?

We support keeping Supplement No. 1 to Part 734. These Q&A have been very helpful to universities and moving them to a website may lessen the effectiveness and force of such guidance.

740.9 Temporary imports, exports reexports, and transfers (in-country) (TMP):

Clarification is requested on paragraph (a)(3)(v). In particular, what document is required? Should the documentation be maintained by the company, or retained by the individual while traveling?

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

“Basic scientific research” uses a name that is not typically found in either the proposed ITAR language (120.49(c)(1)), nor in language used by government administrations (NSDD-189, etc.) We recommend striking the word “scientific”. Furthermore, if “basic research” is defined in 772.1, it would seem appropriate for “applied research” and “fundamental research” to also be defined.

The definition for “Peculiarly responsible” includes both the term “use” as well as “operation, installation, maintenance, repair, overhaul, or refurbishing”. Although the latter is no doubt listed to cover 600 series items, it appears redundant for the definition to be stating “operation, installation, maintenance, repair, overhaul, and refurbishing, ‘operation, installation, maintenance repair, overhaul, or refurbishing.’” We recommend clarifying the need for this distinction perhaps by stating that the specific addition of “operation, installation, maintenance, repair, overhaul, or refurbishing” only applies to 600 series items.

The definition for “technology” should also be modified as recommended for “Peculiarly responsible” above.

Effective date of the final rule:

We support a six-month lead time for implementation of the final rule. The proposed changes to the definitions will require compliance personnel to revise training materials, in some cases implement new procedures, and may require significant consultation with other groups in the organization.

Sincerely,



Mark Stomski
Director of Export Controls

July 31, 2015

Bureau of Industry and Security
U.S. Department of Commerce
14th Street and Constitution Avenue, N.W.
Washington, D.C. 20230
Submitted electronically at publiccomments@bis.doc.gov

Re: Response to Proposed EAR Changes (BIS-2015-0019; RIN 0694-AG32)

Dear Ms. Hess:

The University of Idaho generally supports the proposed EAR changes with some comments. The University is the state's land-grant research university. It engages in extensive research activities, often sponsored by industry partners and involving proprietary information. In addition to its general statement of support, the University has provided a response to the eight issues solicited by BIS for comment, which greatly mirrors the comments provided by Association of American Universities and the Council on Government Relations—

1. Whether the proposed revisions create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR.

Response: There are a number of inconsistencies between the EAR and ITAR which are either relatively minor or reflect longstanding practices. However, there is a major disconnect with regard to prepublication review to assure publication would not divulge a sponsor's proprietary information. EAR 734.8 continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published." ITAR 120.49 states that technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data without any restriction or delay, including research sponsor proprietary information review. It is common practice for company sponsors to require proprietary information review. The effect of the ITAR provision is to remove any research

projects involving defense articles subject to such review from fundamental research. This will have a chilling effect on innovation and University-industry partnerships. No explanation is provided as to the reason for the different policies. The University strongly opposes the proposed change to the ITAR that would now exclude any research subject to prepublication review from being considered fundamental research and urge that the ITAR be aligned with the EAR interpretation and definition of fundamental research.

Another point of difference is the provisions related to government-sponsored research covered by contract controls (EAR 734.11). The proposed EAR rule essentially restates the current 734.11(a), which universities have found confusing. The University prefers the ITAR language at 120.49(b) Note 3, suitably modified to apply to technology arising during or resulting from fundamental research. The examples in 734.11(b) are helpful and should be retained.

A change in the proposed EAR rule of particular relevance to educational institutions is the proposed restatement of the "educational exemption" in the current EAR 734.9, which is removed and reserved. The new statement in the proposed EAR 734.3(b)(3)(iii) merges current ITAR (120.10(b)) and EAR text to state "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." The University suggests that the "and" be changed to "or" to avoid unintentionally limiting this section, i.e., to clearly cover a new university course in an emerging technology area so long as it is included in a course catalog.

2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted.

Response: The proposed alternative definition would read: "Fundamental research" means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." This appears to restate the current definition in a shorter fashion, and on its face we do not see a sharp distinction. However, there may be some vagueness in the term "non-proprietary." Also caution perhaps should be exercised in changing a definition that has been endorsed by a series of Administrations and that has served the scientific community well.

Currently the EAR (§734.3(b)(3)), states that "publicly available technology and software...[that] arise during, or result from, fundamental research" are not subject to the EAR. Under the proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is "intended to be published" would not be subject to the EAR. The proposed rule preamble refers to a proposed note "to clarify that software and commodities are not 'technology resulting from fundamental research.'"

This change would significantly complicate and restrict university research. While natural-language documents written by a researcher would be "technology" that could be freely shared as arising during fundamental research, a computer-language document written by the same researcher, working on the same project (a program in source code), would be subject to deemed export restrictions. "Software" resulting from university research is "published" as well as "technology," as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology. The University strongly recommends that software arising during, or resulting from, fundamental research should not be subject to the EAR.

The University also notes with concern that the current presumption in EAR 734.8(b) that university-

based research will be considered fundamental research appears to have been eliminated. There is no clear policy reason stated for this change. The applicability should continue to be determined by the other criteria in 734.8(b). The University urges BIS to restate the presumption in the final rule.

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

Response: The EAR changes also include definitions of "basic research" (734.8, currently found at EAR 772.1) and "applied research" (drawn from DFARS 31.205-18). The suggested alternate definition of applied research is taken from OMB Circular A-11: "Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met." The University prefers the DFARS definition proposed in 734.8(c)(2) since it is already established in the DFARS and, to our knowledge, has not previously raised concerns.

4. Whether the questions and answers in existing Supplement no. 1 to part 734 proposed to be removed (to the BIS website) have criteria that should be retained in part 734.

Response: the Q&A's have been very helpful to the universities. They are unlikely to have the same weight if removed from the EAR and placed on the website. The University also notes that supplements to other parts of the EAR contain important regulatory information (e.g., Supplement No. 1 to Part 740).

5. With respect to end-to-end encryption as described in the proposed rule (sec. 734.18), whether the illustrative standard in the proposed EAR rule also should be adopted in the ITAR; whether the safe harbor standard in the proposed ITAR rule also should be adopted in the EAR, or whether the two bodies of regulations should have different standards.

Response: The University appreciates that the proposed rules address cloud computing situations, which have been an area of considerable uncertainty under the current rules. BIS asks for comments as to which proposed rule more clearly describes the intended control. The University prefers the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, the University believes that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur.

In addition, the restriction in 734.18(a)(4)(iv) to countries not listed in Country Group D:5 unfortunately may substantially limit the usefulness of the proposed rule. The University suggests BIS consider adding a note that a contract that imposes these obligations on a vendor is sufficient for compliance purposes, to provide a greater safe harbor. Ensuring actual compliance is beyond a university's control.

6. Whether encryption standards adequately address data storage and transmission issues.

Response: The University has no comment on this issue.

7. Whether the proposed definition of "peculiarly responsible" effectively explains how items may be "required" or "specially designed" for particular functions.

Response: These definitions appear reasonable.

8. The effective date of the final rule.

Response: BIS proposes a 30-day delayed effective date. Changes to ECCNs generally have had a six-month delayed effective date while other rules affecting export controls have been effective on the date of publication. Obviously the content of the final rule is an important consideration. Significant changes in definitions should have as long a lead time as possible for implementation. Therefore, the University supports a six-month delayed effective date.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Smith". The signature is fluid and cursive, with a large, stylized initial "R" and a distinct "S" at the end.

Robert Smith, Ph.D.

Senior Associate Vice President for Research and Economic Development
University of Idaho



OFFICE OF THE VICE PRESIDENT - RESEARCH AND GRADUATE STUDIES

Research Policy Analysis and Coordination
1111 Franklin Street, 11th Floor
Oakland, California 94607-5200
Web Site: www.ucop.edu/research/rpac/
Tel: (510) 587-6031
Fax: (510) 987-9456

August 3, 2015
(email to publiccomments@bis.doc.gov)

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
14th Street and Pennsylvania Avenue NW, Room 2099B
Washington, DC 20230

RE: RIN 0694-AG32

Dear Sirs/Madams,

The University of California (UC) system, consisting of ten research-intensive campuses and involved in the management of three DOE national laboratories, applauds the efforts undertaken by agencies committed to supporting the President's Export Control Reform initiative. Specifically, we applaud the Department of Commerce, Bureau of Industry and Security's (BIS) efforts to provide greater clarity of terms used in the Export Administration Regulations (EAR) and the harmonization of these definitions with the International Traffic in Arms Regulations (ITAR).

We believe many of the proposed definitions are certainly meeting the objectives of the Export Control Reform initiative. For example, the notes to §734.3(b) more clearly lay out which items are not subject to the EAR. The comments below are primarily requests for greater precision, both in new definitions and in areas that have historically been a source of confusion.

In addition to the specific comments provided below, UC generally supports the remarks submitted by the Council on Governmental Relations (COGR) and Association of University Export Control Officers (AUECO).

§734.15 Release

We note that the preamble to the proposed changes clearly explains what is meant by §734.15: principally that "merely seeing an item briefly is not necessarily sufficient to constitute a release." It would be useful if this same type of clarity were provided in the definition itself, or alternatively as a note to the section. The term "actually" is used in the preamble as well, but we believe the term "substantively" would be more precise. Thus, borrowing from the definition of technology, a recommended rewrite of this section is:

(1) Visual or other inspection by a foreign national of items that substantively reveals “technology” or “source code” sufficient to enable the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control “technology”) of an item.

§734.3(b)(3)(iii) (Not subject to the EAR)

UC appreciates the clarification in the note to paragraph (b)(3) that information that is not “technology” as defined in the EAR is not subject to the EAR. With regard to subsection (iii), although we recognize the clause “general scientific, mathematical, or engineering principles commonly taught in schools” has been used in the ITAR for many years, we would recommend that the terms “general” and “commonly” be removed from this definition. Indeed, core to the University’s mission is to teach and involve students in knowledge (and in the pursuit of knowledge and innovation) beyond “general” or “common” introductory coursework. Although we do not think that the intent was ever to limit this exclusion to general basic coursework, removal of these terms would resolve potential ambiguity. Thus, we recommend §734.3(b)(iii) be modified to read:

“(iii) Concern scientific, mathematical and engineering principles, processes, and techniques taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution;”

§734.11 Government-sponsored research covered by contract controls and 734.8 Fundamental Research

The proposed §734.11 reads:

(a) If research is funded by the U.S. Government, and specific national security controls are agreed on to protect information resulting from the research, the provisions of §734.3(b)(3) will not apply to any export or reexport of such information in violation of such controls. However, any export or reexport of information resulting from the research that is consistent with the specific controls may nonetheless be made under this provision.

(b) Examples of “specific national security controls” include requirements for prepublication review by the Government, with right to withhold permission for publication; restrictions on prepublication dissemination of information to non-U.S. citizens or other categories of persons; or restrictions on participation of non-U.S. citizens or other categories of persons in the research. A general reference to one or more export control laws or regulations or a general reminder that the Government retains the right to classify is not a “specific national security control.”

We recognize that this section essentially remains the same; however because it has been a source of confusion, we request greater clarity about the meaning of this section, specifically, whether/how agreeing to “specific national security controls” of the type listed in §734.11(b) affects the status of research that would otherwise be considered “fundamental research.”

Such clarification would be especially welcome given that the reference to §734.11 in §734.8 has been changed. Currently, §734.8(a) states that fundamental research is distinguishable from research the results of which ordinarily are restricted for specific national security reasons as defined in §734.11(b). This has been understood by many to mean that accepting controls such as those listed in §734.11(b) (including restrictions imposed by the U.S. government on participation of non-citizens or other categories of persons in the research, as well as publication restrictions) would take research subject to those controls out of the fundamental research exclusion. Under the proposed revision, the reference to §734.11 has been moved to Note 2 of §734.8(b), which states that *except as provided in §734.11*, technology subject to *publication restrictions* such as U.S.

government-imposed *access and dissemination controls* is not “intended to be published” (which means it would not qualify as fundamental research). We think it is important for the BIS to clarify:

- (1) Which types of controls negate categorization of research as fundamental? That is, is it only *publication restrictions* controlling access to and dissemination of *results* that would take research outside of the fundamental research exemption, as is suggested by the language of §734.8 as it is proposed to be amended? Or, conversely, would the same consequence result from acceptance of restrictions on *participation* in the research project itself (i.e., where there are no restrictions on publication), given that §734.11(b) specifically lists such participation controls as an example of “specific national security controls”?
- (2) Whether/how the effect of accepting such controls is different depending on whether the controls are imposed by U.S. Government or by a non-governmental sponsor of research. Because §734.11 applies only to research funded by the U.S. Government, some might conclude that institutions have more leeway to accept controls from U.S. Government sponsors than from non-governmental sponsors (as long as they comply with the accepted controls) without entirely negating the classification of the research as fundamental research, but the meaning of the section is confusing.
- (3) Whether/how agreeing to “specific national security controls” with respect to U.S. Government-funded research affects the status of research that would otherwise qualify as “fundamental research.” For example, if we accept and comply with “specific national security controls” imposed by a U.S. Government funder (such as citizenship restrictions or foreign national prior approval requirements), would acceptance of those controls negate the fundamental research exclusion? Or, does §734.11(a) mean that the project could be conducted as fundamental research, that is, with no export licensing required, as long as we complied with the government imposed citizenship restrictions or foreign national prior approval requirements? Or, are such projects considered controlled by the EAR only *during* the conduct of the research?

We would appreciate revisions to this section to clarify the intent of the clause.

§734.8 Technology that arises during, or results from, fundamental research

In addition to the comments made above with regard to the connections between §734.11 and §734.8, we have the following comments on §734.8. First, we appreciate that §734.8(a) retains the notion that technology that arises during, or results from, fundamental research is “intended to be published” and thus not subject to the EAR. However, we note that “software” is missing from this paragraph, even though it is included in the proposed definitions at §734.3(b)(3) and §734.7(a). There is no apparent reason to treat software differently from technology and request its reinsertion at §734.8(a).

UC also appreciates that §734.8(b) continues to recognize that prepublication review to assure that a sponsor's proprietary information is not divulged or that the publication does not compromise patent rights is still “intended to be published.” The currently proposed ITAR definitions, in contrast, do not have the same protections provided by paragraph (b). This is a great concern to the university community, and has been communicated to the Department of State.

With regard to §734.8(c), UC appreciates the clarifications provided in the fundamental research, basic research, and applied research definitions. We believe these do not contradict the intent of National Security Decision Directive 189. BIS requested comments on whether the proposed definition for basic research is preferable to the definition contained within Office of Management and Budget Circular A-11. UC prefers the definition in the proposed regulations, as this definition is consistent with the current EAR definition, the ITAR proposed definition, and with the Wassenaar Arrangement’s General Technology Note:

(1) “Basic research” means experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective.

In addition, we recommend the addition of a note to §734.8(c) to clarify that academic prototypes and mock-ups which originate under a fundamental research project and are not intended for commercial use, are considered to be within the definition of “applied research.”

§734.18 Activities that are not exports, reexports, or transfers

UC welcomes the consolidation into a single provision of existing EAR exclusions from exports, reexports, and transfers and the addition of end-to-end encryption at §734(a)(4)(iv). However, we request a definition for “storage” to assure that exports currently allowed with the use license exceptions would still be permitted. For example, if a U.S. person using a temporary export license exception travels with their laptop computer to a D:5 country, their possession of the laptop computer while in the D:5 country should not be considered “storage.” Furthermore, electronic transmissions (such as email) of technology subject to the EAR transiting through a D:5 country or the Russian Federation that would otherwise meet the conditions of this provision, should likewise not be considered “storage” if the sender does not know that the email server is located in a D:5 country or in the Russian Federation.

Supplement no. 1 to Part 734

BIS requested comments on whether the questions and answers currently incorporated into Part 734 as a supplement should be extracted from the regulations and posted on the BIS website. UC urges the continued incorporation of these as a supplement. A posting on the BIS website would not provide the same weight, and we believe that the questions and answers should be fairly static. Furthermore, the public should be provided with the opportunity to comment on alterations to the answers. If they are posted on the BIS website, the public would not necessarily be consulted on subtle or substantive changes, potentially impacting existing compliance procedures implemented by businesses and universities alike.

Implementation

Finally, UC would like to request a 6 month implementation period for the revised definitions of this proposed rule to allow for proper analysis of business practices and modifications as appropriate.

Thank you for this opportunity to comment. We greatly appreciate your efforts to seek input regarding the EAR Amendment—Revisions to Definitions in the Export Administration Regulations and are in the main supportive of the clarifications made in these proposed definitions.

Sincerely yours,



Wendy D. Streit
Executive Director
Research Policy Analysis & Coordination
Office of Research & Graduate Studies



PAUL HORN
Senior Vice Provost for Research

Office of the Provost
70 Washington Square South, rm 1228
New York, NY 10012
P: 212 998 3228
paul.horn@nyu.edu

Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230
Subject: RIN 0694-AG32

Dear Ladies and Gentlemen:

We are writing to comment on the proposed revisions to the EAR. We applaud the goal of harmonizing the EAR with the ITAR and in large measure agree that this goal has been met. In addition, we have reviewed the AAU/APLU/COGR response to you and agree with all of the points contained therein.

We wish to highlight a few areas which are of particular concern to New York University as a major research university. A major inconsistency has arisen between the proposed EAR and ITAR regulations with the latter stating that sponsor review of proprietary information removes it from “fundamental research”. We have indicated in our comment letter to the DDTTC that their provision would have a chilling effect on innovation and university-industry partnerships and directly works against the Administration's efforts which have sought to increase university-industry collaboration and move new ideas quickly from the lab to the marketplace. The proposed ITAR provision would impede the ability of universities to achieve these objectives, particularly in defense-related areas where universities often serve as subcontractors to defense contractors for research related to particular defense technologies. It is hard to see how this serves our national security interests and we would argue that it clearly does not serve our economic interests. We strongly prefer the EAR version in 734.8 to the ITAR 120.49(b).

Under the proposed 15 CFR 734.8(a), software was removed. Therefore, while natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions. “Software” resulting from university research is “published” as well as “technology”, as recognized in the current 15 CFR 734.7(b). The export definitions in 15 CFR 734.2(b) recognize the similarities between software and technology. We recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.

As the AAU/COGR/APLU letter states, another point of difference in the provisions is related to government-sponsored research covered by contract controls (EAR 734.11). The proposed EAR rule essentially restates the current 734.11(a), which universities have found confusing. We prefer the ITAR language at 120.49(b) Note 3, suitably modified to apply to technology arising during or resulting from fundamental research. The examples in 734.11(b) are helpful and should be retained.

The removal of the specific criteria for university-based research currently found in 15 CFR 734.8(b) creates interpretive uncertainty in the new proposed definitions. Universities use this regulation to

make determinations as to the applicability of fundamental research by evaluating proposed research activities using paragraphs 2-6, and assuming that the research qualifies as “fundamental research” if all conditions are met. The development of a decision tree tool for the determination of fundamental research for universities that incorporates the current criteria for university-based fundamental research would be most helpful.

A change in the proposed EAR rule of particular relevance to NYU as an educational institution is the proposed restatement of the "education exemption" in the current EAR 734.9, which is removed and reserved. The new statement in the proposed EAR 734.3(b)(3)(iii) merges current ITAR (120.10(b)) and EAR text to state "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." We suggest that the "and" be changed to "and/or" to avoid unintentionally limiting this section, i.e., to clearly cover a new university course in an emerging technology area so long as it is included in a course catalog.

The addition of 15 CFR 734.18 which lists activities that are not exports, re-exports or transfers is a useful addition to the EAR. In particular, the exclusion of sending, taking, or storing software that is secured using end-to-end encryption from export activities is welcome to the academic research community as it will reduce the faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. The proposed EAR illustrative standard of FIPS 140-2 supplemented in accordance with NIST guidance or other similarly effective means is also quite helpful.

We believe that the Q&A in Supplemental no 1 to part 734 should be retained. While the Q&A is illustrative, including them in the EAR removes the uncertainty created by changes due to interpretive differences without the benefit of the rulemaking process. Removal would result in an increased uncertainty in the application of key concepts including fundamental research, publication, and educational instruction.

We appreciate the opportunity to comment on these proposed new definitions and thank you for your willingness to continue the dialogue on these important issues.

Sincerely,

Paul Horn
Senior Vice Provost for Research



Perspecsys Inc.
1750 Tysons Blvd., Suite 1500
McLean, Virginia 22102

August 3, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Re: Response to Request for Comments Regarding Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32) – Use of Tokenization to Secure Technology in the Cloud

On June 3, 2015, the Bureau of Industry and Security (BIS) issued a Federal Register notice requesting comments on proposed amendments to the Export Administration Regulations (EAR, 15 C.F.R. Parts 730 – 774) that would revise certain definitions and update controls on the transmission and storage of technology in the cloud.¹

PerspecSys Inc. (PerspecSys or the Company) respectfully submits these comments on the proposed definition of activities that are not exports, reexports or transfers (proposed § 734.18) and the revised subsection of license exception TMP regarding exports of technology to U.S. persons (§ 740.9(a)(3)).

In sum, PerspecSys supports amending the EAR to allow the secure transfer and storage of obfuscated technology in the cloud pursuant to the proposed § 734.18, but suggests that clarifying changes be made to §§ 734.18 and 740(a)(3) indicating that tokenization is an acceptable data obfuscation method in addition to encryption. According to many data security experts, tokenization provides data obfuscation, security, and operational functionality that is stronger than or as strong as encryption-only systems when implemented properly. Tokenization should therefore be explicitly recognized in the regulations as an approved data obfuscation method.

1. Company background

¹ Proposed Rule, Revisions to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31505, 31517 (June 6, 2015).

PerspecSys provides cloud data control and security solutions to protect customers' sensitive information before it leaves their networks. In particular, PerspecSys' tokenization process allows customers to utilize cloud applications to process sensitive data without actually moving that sensitive data to the cloud. This process ensures data residency (e.g., that data remains on companies' secure network in the U.S.) and reliable obfuscation (e.g., there is no way to determine the clear text of the controlled data based on the information that is transmitted to the cloud).

2. Tokenization background

Tokenization is a process through which controlled or sensitive data or documents are obfuscated by replacing underlying clear text with a surrogate value called a "token." Tokens are used as reference or lookup values for underlying clear text or documents that are marked as sensitive by the data owner. Tokens are arbitrarily generated strings of characters with no mathematical or logical association to the clear text they replace or the documents they reference. PerspecSys tokens are generated and assigned through a sequentially generated and randomly assigned process (an important methodology distinction that will be discussed later in the request).

PerspecSys tokenization is used at the document and the field level.² Multiple tokens may be used for the same value depending on how narrowly or broadly a user sets "token spaces." Users of PerspecSys tokenization can define the scope of data that will share the same token for the same clear text data.³ Users may also rotate token spaces over time so that a new set of tokens are assigned to data generated after a certain date.⁴

A "token vault" is a reference database containing a list of all tokens used and the corresponding clear text value. The token vault is maintained within the data owner's secured network and is encrypted for additional protection. PerspecSys' tokenization process occurs within a customer's secured network. Companies utilizing tokenization to protect EAR-controlled technology would treat the token vault as controlled and ensure that it is secured in compliance with EAR requirements (e.g., ensure that the token database is stored in an authorized country and secured from access by unauthorized persons).

Tokens are then transmitted to cloud providers for processing or storage.

² For example, a technical drawing would be replaced by a token value such as "prs_rky5433_z." That token would serve as a reference to the actual drawing (sometimes referred to as a "pointer token"), but would contain no information about the drawing. The token would then be transferred to the cloud, but the underlying drawing would remain locally stored within the data owner's secured network. Similarly, a unique field value in an enterprise resource planning (ERP) system (e.g. "John Smith" as the bill to party for a transaction) would be assigned an arbitrary token value such as "prs_AHJucx3_z." Again, the token value may be transmitted to the cloud, but the underlying "John Smith" value would not be transferred from the data owner's network. Data that is flagged as being non-controlled would pass through the system as clear text.

³ For example, a user may specify a different token space be used for each field in an ERP system. As a result, "John Smith" as the "bill to" party may be represented by a token value of "prs_AHJucx3_z," while "John Smith" as the "ship to" party may be represented by a token value of "prs_KL3txL_2."

⁴ As a result, "John Smith" as the "bill to" party may be represented in an ERP system by one token for a transaction on day 1, a second token on day 2, and a third token on day 3, and so on.

3. Security and data obfuscation advantages of tokenization

Tokenization, when implemented properly and at an appropriate security level as part of a comprehensive data security system,⁵ provides distinct security advantages over data obfuscation methods based solely on encryption. Of course, not all forms of tokenization would be sufficient to properly secure technology in the cloud, just as not all forms of encryption are sufficient to secure data from unauthorized access. To secure controlled technology in the cloud, tokens must be non-authenticable and irreversible tokens.⁶

There is no way to mathematically “break” or derive the plain text of such strongly tokenized data without access to the token vault, which would be secured with other controlled data (or secured at an even higher level) within an encrypted database on a secured enterprise/agency datacenter in the United States. Furthermore, knowing the clear text or document associated with one or more tokens provides no insight to the clear text or document associated with any other token because tokens are not mathematically linked. In contrast, encrypted data stored on the cloud can be decrypted through the use of a key or through mathematical derivation (i.e., “breaking” the encryption). Furthermore, once the key to the encryption algorithm is obtained, all data encrypted using that algorithm may be decrypted. Failing to permit the use of tokenization to secure controlled technology would provide an unwarranted commercial advantage to one data security approach when an equivalent or superior technique provides the same or better security.

When tokenization is utilized, the underlying controlled technology would never be exported. The clear text of the underlying technology would be stored locally within the owner’s secured network. The underlying data would never leave the owner’s control in any format, either in clear text or in a mathematically derivable form. As a result, there can be no incidental export of the controlled technology, because only the replacement token value would be moved to the cloud (and potentially exported by cloud computing service providers).

⁵ For example, such a system would include the following elements: (1) Controlled technology would be secured in the U.S. on servers restricted from foreign national access; (2) Tokens must be generated in such a way as to prevent any link between the clear text data and the token, including, for example, assignment of tokens through an index function or randomly generated number. A mathematically reversible cryptographic function would not be sufficient. (3) The entire tokenization system (including token generation, the tokenizing and de-tokenizing processes, token mapping, data vault and cryptographic management) should be housed in the U.S. and subject to security requirements at least as stringent as those applied to controlled technology (and likely far more restricted). PerspecSys secures the tokenization system using FIPS 140-2 encryption within an enterprise’s or agency’s secured network. (4) Additional best practices would include strong authentication and access controls, robust monitoring, and commination controls between the tokenized database and third party applications.

⁶ See [Tokenization Product Security Guidelines](https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf), PCI Security Standards Council, April 2015, p. 7, available at: https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf.

In addition, tokenization eliminates the need for complex key management procedures, which are costly to implement in a cloud environment and, if not properly controlled, are a potential security concern.⁷

4. Suggested revisions to the proposed Sec. 734.18(a)(4)

Given the potential advantages of using tokenization to secure controlled technology in the cloud, PerspecSys suggests that the proposed definition at § 120.52(a)(4) be modified to include tokenization as a permissible data security methodology. Specifically, PerspecSys suggests that the following changes be made to the proposed rule (bolded):

(a) * * *

(4) Sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption **or tokenization**;

(iii) Secured using **cryptographic data obfuscation** modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and

(iv) Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation.

(b) Definitions. For purposes of this section, ‘end-to-end encryption **or tokenization**’ means the provision of uninterrupted **cryptographic obfuscation** of data between an originator and an intended recipient, including between an individual and himself or herself. It involves **encrypting obfuscating** data by the originating party and keeping that data **encrypted obfuscated** except by the intended recipient, where the means to access the data in unencrypted **or clear text** form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access “technology” or “software” in **encrypted obfuscated** form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such “technology” or “software.”

⁷ See SecaaS Implementation Guide, Category 8, Cloud Security Alliance, p. 18-19, available at: <https://cloudsecurityalliance.org/download/secaas-category-8-encryption-implementation-guidance/>.

These changes would allow industry to implement data security solutions incorporating tokenization methodologies that, when implemented properly, provide advantages over encryption-based data obfuscation systems.

5. Suggested revisions to clarify the amendment of Sec. 740.9(a)(3)

PerspecSys suggests that the proposed amendment to § 740.9(a)(3) be clarified to indicate that encryption and tokenization may be used to secure data pursuant to the exemption. As BIS is aware, tokenization and cryptography are distinct methods for obfuscating data. The current proposal lists encryption as an illustrative example of required security precautions, but does not reference tokenization, or more generally, data obfuscation. While the current language does not necessarily preclude the use of tokenization to comply with § 740.9(a)(3), it may create confusion among industry on which data security measures to adopt when securing controlled technology in the cloud.

As the BIS is aware, the Directorate of Defense Trade Controls (DDTC) issued an advisory opinion and related correspondence to PerspecSys indicating that tokenization may be used to secure ITAR-controlled technical data pursuant to the exemption in 2014.⁸ The Company requests that the amended § 740.9(a)(3) include a similar reference to tokenization for the export of EAR-controlled technology to U.S. persons abroad.

Specifically, PerspecSys suggests that the following changes be made to the proposed rule (bolded):

(a) * * *

(3) “Technology,” regardless of media or format, may be exported by or to a U.S. person or a foreign national employee of a U.S. person, traveling or on temporary assignment abroad, subject to the following restrictions:

(i) Foreign nationals may only export or receive such “technology” as they are authorized to receive through a license, license exception other than TMP or because no license is required.

(ii) “Technology” exported under this authorization may only be possessed or used by a U.S. person or authorized foreign national and sufficient security precautions must be taken to prevent the unauthorized release of the “technology.” Such security precautions include **obfuscation (i.e., through encryption or tokenization)** of the “technology,” the use of secure network connections, such as Virtual Private Networks, the use of passwords or other access restrictions on the electronic device or media on which the “technology” is stored, and the

⁸ See DTC Case No. GC 0317-14 (Feb. 5, 2014) (“tokenization may be used to process controlled technical data using cloud computing applications without a license even if the cloud computing provider moved tokenized data to servers located outside the U.S., provided sufficient means are taken to ensure the technical data may only be received and used by” authorized persons).

use of firewalls and other network security measures to prevent unauthorized access.

(iii) The U.S. person is an employee of the U.S. Government or is directly employed by a U.S. person and not, e.g., by a foreign subsidiary.

(iv) Technology” authorized under this exception may not be used for foreign production purposes or for technical assistance unless authorized through a license or license exception other than TMP.

(v) The U.S. person employer of foreign nationals must document the use of this exception by foreign national employees, including the reason that the “technology” is needed by the foreign nationals for their temporary business activities abroad on behalf of the U.S. person.

6. Conclusion

PerspecSys appreciates BIS’s and other agencies’ consideration of our comments. Tokenization can offer reliable data obfuscation and data security sufficient to protect controlled technology in the cloud. We encourage the agency to revise the proposed amendments to specifically include tokenization as a valid data obfuscation methodology to encourage industry to adopt solutions that will best protect their data while it transits through overseas networks.

* * *

Please contact the undersigned at 703-712-4752 or gerry.grealish@Perspecsys.com with any questions or for additional information.

Sincerely,

Gerry Grealish
CMO, Perspecsys



Office of the Vice Chancellor
for Research and Graduate Education
UNIVERSITY OF WISCONSIN-MADISON

August 3, 2015

Department of Commerce
Bureau of Industry and Security
Washington, DC
By email to publiccomments@bis.doc.gov

RE: RIN 0694-AG32
15 CFR 734, 740, 750, 764, and 772

Dear Sirs/Madams:

Please accept the following comments from the University of Wisconsin-Madison (UW-Madison) in response to the Department of Commerce Proposed Rule for *Revisions to Definitions in the Export Administration Regulations*. UW-Madison endorses the comments submitted jointly by the Association of American Universities (AAU), the Council on Governmental Relations (COGR), and the Association of Public Land Grant Universities (APLU); we are a member of those associations. As one of the largest public research institutions in the United States, with approximately a billion dollars in annual research expenditures, a broad research portfolio, a strong international presence, and a large number of international students, staff and visitors, UW-Madison believes it is critical that export control laws strike an appropriate balance between the free interchange of scholarly information and the advancement of science, and the protection of national security and economic competitiveness. We appreciate and support the efforts of the Departments of Commerce and State to harmonize the definitions among the EAR and ITAR, and there have been a number of positive outcomes from this process. However, it is important that this progress continue, and UW-Madison is greatly concerned that certain provisions in the above-referenced proposed rules represent a reversal of the overall positive trend of export control reform.

Please allow us to identify the items of most concern.

- **Inconsistent treatment of pre-publication review by a research sponsor under EAR and ITAR.** EAR 734.8 continues to provide that pre-publication review by a research sponsor for a limited time to identify proprietary information or to enable intellectual property protection does not change the status of technology that arises during or results from fundamental research as still "intended to be published" and thus not subject to the EAR. However, under the companion ITAR proposed rule, ITAR 120.49 would state that technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical data without any restriction or delay, including research sponsor proprietary information review. The effect of the proposed ITAR provision is to effectively preclude any

industry-funded research involving defense articles from treatment as fundamental research, which will greatly hinder innovation and university-industry partnerships, and constrict the transfer of University technology to the private sector.

There a number of reasons why an industrial sponsor might request a brief delay in publication. In addition to providing industrial sponsors a brief window of time to ensure that their proprietary business information is not inadvertently revealed in a publication, industrial sponsors request publication delays to ensure sufficient time to file patent applications, to ensure that descriptions of company activities referenced in manuscripts are accurate, and to allow for the joint publication of collaborative research occurring in multiple sites. Federal government sponsors also frequently request pre-publication review so they can be alerted to the content of impending publications, ensure that federal support is properly attributed, permit the orderly publication of collaborative research, etc. No explanation is provided as to the reason for the proposal for different policies.

We strongly oppose this proposed change to the ITAR that would now exclude any research subject to prepublication review from being considered fundamental research. We urge that the ITAR be aligned with the EAR interpretation and definition of fundamental research.

- **Exclusion of software and commodities from treatment as “technology resulting from fundamental research.”** Under current law, “publicly available technology and software... [that] arise during, or result from, fundamental research” are not subject to the EAR. Consistent with current law, under the proposed §734.8(a), “‘technology’ that arises during, or results from, fundamental research and is ‘intended to be published’” would not be subject to the EAR. However, the proposed rule preamble refers to a proposed note “to clarify that software and commodities are not ‘technology resulting from fundamental research.’” This proposed change makes no sense, and would appear to impose export controls for the first time on such things as government-funded open source distributed network computing software including UW-Madison’s HTCondor software, as well as the many smartphone “apps” being developed for teaching and research purposes. As noted in the AAU/COGR/APLU comments, software is simply a form of written language, and it is illogical to treat software differently from other written forms of information irrespective of what the software does or how it is disseminated.

Similarly, excluding commodities from “technology resulting from fundamental research” without regard to the nature or purpose of the commodity or the circumstances under which it was developed would impose controls on a wide range of innocuous devices with no apparent benefit to national security of economic competitiveness. For example, it is very common for simple devices to arise from fundamental research projects, where all information necessary to assemble the device is openly shared, such as enrichment devices which are created to enhance the comfort of laboratory animals.

Finally, we note that this proposed exclusion of software and commodities from “technology resulting from fundamental research” conflicts with proposed EAR 734.8 Note 1 to paragraph (a), which states: “The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technology that arises during or results from fundamental research” except to the extent that such inputs are technology that arose during or resulted from earlier fundamental research.”

We ask that you do not exclude software and commodities from “technology resulting from fundamental research.”

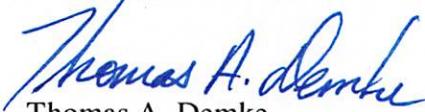
- **The description of educational activities not subject to the EAR is unclear and open to broad variations in interpretation.** The word “general” is included, but not defined, in EAR 734.3(b)(3)(iii) to qualify “scientific, mathematical, or engineering principles commonly taught in schools.” The proposed wording can be interpreted to mean only entry-level courses. This would severely inhibit ability of universities to develop new upper-level and advanced courses in the competitive fields of engineering and science for fear that what is taught in them would not be considered “general.” Such wording has also previously been interpreted to exclude capstone classes, something that is part of normal coursework for a large number of students. “Commonly taught” is also an inexact phrase subject to great variations in interpretation as different universities have different subject areas in which they are leaders. Narrow application of these terms would severely restrict educational activities.

We suggest retaining the current definition of “educational information” under 734.9 (“information released by instruction in catalog courses and associated teaching laboratories of academic institutions”). If this is not possible, we recommend deleting the word “general” from the proposed definition.

- **General Comment regarding Effective Date.** The proposed changes would require that we review university contracts to ensure compliance, a task that will take more than 30 days. We suggest changing the effective date from 30 days from publication to 180 days from publication. Six month effective dates have been used previously following revisions of some export control rules.

The University of Wisconsin-Madison appreciates the opportunity to provide the Department of Commerce with the above comments. We believe that the laudable effort to harmonize the export control laws should not serve to weaken the essential protections for the results of university-based fundamental research which are so critical to the ability of universities to meet the research needs of the private sector while still maintaining an open research environment that is essential to the education of students, the ability to forge international collaborations, and the creation of innovative technologies.

Sincerely,



Thomas A. Demke
Export Control Officer



Dan Uhlrich
Associate Vice Chancellor for Research Policy



Operating under the joint auspices of:



**c/o ADS
"ShowCentre"
ETPS Road
Farnborough
Hampshire GU14 6FD
United Kingdom**

Tel: +44 20 7091 7822

Fax: +44 20 7091 4545

E-Mail: Brinley.Salzmann@adsgroup.org.uk

URL: www.egad.org.uk

28 July 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B, 14th Street and Pennsylvania Ave. NW
Washington DC 20230
United States of America
publiccomments@bis.doc.gov

RIN 0694–AG32: Revisions to Definitions in the Export Administration Regulations

Dear Sir,

I write to you on behalf of the Export Group for Aerospace and Defence (EGAD), which is a not-for-profit making special interest industry group, focusing exclusively on all aspects of export and trade control compliance matters, and is the only dedicated national industrial body in the UK dealing exclusively with export and trade control issues. EGAD operates under the joint auspices of the ADS Group Ltd (ADS), British Marine, the British Naval Equipment Association (BNEA), the Society of Maritime Industries (SMI), and TechUK.

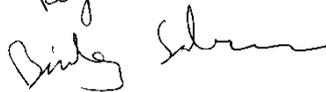
This is in response to the consultations which were launched by the US Government on Wednesday 3rd June 2015, seeking comments on proposals for revisions to the Export Administration Regulations (EAR) to include the definitions of "technology", "required", "peculiarly responsible", "proscribed person", "published", results of "fundamental research", "export", "re-export", "release", "transfer", and "transfer (in-country)" to enhance clarity and consistency with terms also found on the International Traffic in Arms Regulations (ITAR), which is administered by the Department of State, Directorate of Defense Trade Controls (DDTC), as part of the on-going US Export Control Reform (ECR) process.

We are grateful for the high degree of constructive engagement, willingness to enter into open discussions and debate, and assistance that the US Government has unfailingly demonstrated on ECR, which have been hugely beneficial.

We would like to state that UK Industry in general is supportive of any and all efforts and initiatives associated with the ECR process to try to provide greater clarity and ease of use of US licensing. We remain committed to try to do all that we can to assist UK Industry in their understanding of the process. However we would like to submit the following comments. They relate exclusively to the new proposals relating to cryptography, set out in EAR 734.18 and the associated 764.2(l). :

- a. We fully endorse the reasoning which has led BIS to propose the addition to FIPS 140-2 of 'other similarly effective cryptographic standards'. We have separately urged DDTC to adopt similar language. As non-US companies, our members operate in multiple jurisdictions. Cybersecurity and data protection are dynamic fields and national policies are constantly changing. There is always the likelihood that our domestic or international jurisdictions, as well as risk management needs, will require the use of an encryption standard that is not formally FIPS 140-2 compliant, but is similarly effective. Here in the UK, for example, companies are required to use the BeCrypt product for certain interaction with the UK Ministry of Defence. Non-US companies may also need to manage ITAR and EAR items and the different encryption rules would make developing a unified system to handle both EAR and ITAR compliance extremely challenging
- b. The transfer of encrypted items in storage to restricted destinations without the owner's knowledge, should not be considered a violation by the owner. The revised EAR §734.18(a)(4)(iv) should address the scenario where properly encrypted data or software stored on a third-party's server, such as a cloud server, is transferred to a restricted jurisdiction without the permission or knowledge of the company utilizing the third party's service. As such, we suggest adding a "knowingly" standard to protect those entities that conducted due diligence in procuring third-party services from providers that do not store technical data or software in a prohibited country but whose data may end up in one of those countries without their prior knowledge or consent.
- c. EAR §734.18(a)(4)(iv) includes a restriction that the unclassified technical data or software cannot be "stored" in the Russian Federation or any country listed in Country Group D:5. However the term "stored" is not defined. One would assume that this means intentional storing of information on a data server for a period of time rather than an email transiting a server and being retained temporarily for this purpose. We urge you to make clear that these country restrictions only apply to ongoing storage and not the possible transit of email through those countries. This is necessary as the sender of a secured email typically has no control over what countries an email has passed through on its way to its final destination – even emails sent between a sender and recipient in the United States may transit a third country.
- d. The proposed EAR §764.2(l) states that the unauthorized release of decryption keys, network access codes, passwords, or other transfer information that would allow access to the encrypted information in clear text is an export control violation. In order to avoid any duplication of licensing, we ask that BIS make clear that existing authorizations for the export, re-export, or retransfer of information also authorize the release of decryption keys, network access codes, passwords, or other transfer information that would give access to that same controlled information to authorized parties on export license approvals. Without this clarification, companies may need to seek two separate authorizations: one that covers the export, re-export, or retransfer of controlled information and one that covers the release of decryption keys, network access codes, passwords, or other transfer information to the same authorized parties.

Thank you in advance for your consideration of these comments. If you have any questions about this correspondence please contact me.

Regards


Brinley Salzmänn - Secretary, EGAD



August 3, 2015

Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Re: RIN 0694-AG32; Proposed Rule on Revisions to Definitions in the Export Control Administration Regulations

To Whom It May Concern:

On behalf of the University of Southern California (USC), thank you for the opportunity to submit comments on the Proposed Rule on Revisions to Definitions in the Export Control Administration Regulations (15 CFR Parts 734, 740, 750, 764, and 772) 22 CFR Parts 120, 123, 125, and 127).

The University of Southern California is one of the world's leading private research universities. In fact, we are among a small group of premier research institutions on which our country depends for a steady stream of new knowledge and technology. USC has nearly \$700 million in annual research expenditures. In FY 2014, approximately \$80 million of that amount was awarded by the Department of Defense (DOD).

In response to BIS' request for feedback on specific issues related to the Proposed Rule, we respectfully submit the following comments:

- 1. Whether the revisions proposed in this rulemaking create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR*

While we are grateful that the Departments of Commerce and State have made noteworthy progress in harmonizing the export control regulations, there is still a significant distinction in the proposed regulations with regard to prepublication review to assure publication does not divulge a sponsor's proprietary information. Under the EAR, Section 734.8 continues to provide that such review does not change the status of technology that arises during or results from fundamental research as still "intended to be published." However, under the ITAR, proposed Section 120.49 provides that such review makes the research ineligible for fundamental research protection. The effect of the ITAR provision is to remove any research projects involving defense articles subject to such review from fundamental research.

Given that sponsor review for the presence of proprietary information is common, such a rule will have a chilling effect on innovation and university-industry partnerships. We strongly oppose this proposed change and urge that the EAR and ITAR be aligned with the EAR interpretation and definition of fundamental research.

2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted.

The proposed alternative definition would read: "Fundamental research' means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community."

While this appears to restate the current definition and does not represent a sharp distinction from the current definition, the term "non-proprietary" may be vague as applied to specific research projects. We believe that the definition in NSDD-189 has served the scientific and research community well, and care should be exercised before modifying it.

In addition, the EAR currently provides that publicly available technology and software that arise during or result from fundamental research are not subject to the EAR. However, under proposed Section §734.8(a), only "technology" that arises during, or results from, fundamental research and is 'intended to be published'" would not be subject to the EAR.

This change would significantly complicate and restrict university research. While natural-language documents written by a researcher would be "technology" that could be freely shared as arising during fundamental research, a computer-language document written by the same researcher, working on the same project (a program in source code), would be subject to deemed export restrictions. We strongly recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

We prefer the DFARS definition proposed in 734.8(c)(2) to the one suggested in the preamble since it is already established in the DFARS and, to our knowledge, has not previously raised concerns.

4. *Whether the questions and answers in existing Supplement No. 1 to part 734 proposed to be removed by this rulemaking have criteria that should be retained in part 734.*

While we believe that the Q&A's are very helpful, they are unlikely to have the same weight if removed from the EAR and placed on the website as guidance and ask that they be retained.

5. *With respect to end-to-end encryption described in the proposed revision of the definition of "Activities that are Not Exports, Reexports, or Transfers," whether the illustrative standard proposed in the EAR rulemaking also should be adopted in the ITAR rulemaking; whether the safe harbor standard proposed in the ITAR rulemaking also should be adopted in the EAR rulemaking; or whether the two bodies of regulations should have different standards.*

We prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national, because in general, we believe that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur.

6. *The effective date of the final rule.*

BIS proposes a 30-day delayed effective date. Previous changes to ECCN's generally have had a six-month delayed effective date and our view is that significant changes in definitions of key terms should have a similar lead time prior to implementation. Therefore, we suggest a six-month delayed effective date for the final rule.

Thank you very much for the opportunity to submit comments to the proposed rule, and for your ongoing efforts to harmonize export control regulations in a way that both supports the mission of research universities and enhances U.S. national and economic security.

Sincerely,



Randolph W. Hall
Vice President of Research

August 3, 2015

Ms. Hillary Hess
Director
Regulatory Policy Division
Room 2099B
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Ave., N.W.
Washington, D.C. 20230

Mr. Ed Peartree
Director
Office of Defense Trade Controls Policy
U.S. Department of State
2401 E Street, N.W.
Washington, D.C. 20037

Re: Revisions to Definitions in the Export Administration Regulations (*Federal Register* Notice of June 3, 2015; RIN 0694-AG32) and International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions (*Federal Register* Notice of June 3, 2015; RIN 1400-AD70)

Dear Ms. Hess and Mr. Peartree:

The Semiconductor Industry Association (“SIA”) is the premier trade association representing the U.S. semiconductor industry. Founded in 1977 by five microelectronics pioneers, SIA unites over 60 companies that account for nearly 90 percent of the semiconductor production of this country. The semiconductor industry accounts for a sizeable portion of U.S. exports.

SIA is pleased to submit the following public comments in response to the request for public comments issued by the Commerce Department’s Bureau of Industry and Security (“BIS”) on proposed revisions to definitions in the Export Administration Regulations (“EAR”),¹ and the request for public comments issued by the State Department’s Directorate of Defense

¹ Revisions to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31,505 (Jun. 3, 2015) (“EAR Harmonization Definitions”).

Trade Controls (“DDTC”) on proposed new definitions and proposed revisions to definitions in the International Traffic in Arms Regulations (“ITAR”).²

I. Introduction

A goal of any regulatory regime should be to streamline and clarify regulations to the greatest extent possible while providing appropriate rules for behavior. The President’s Export Control Initiative is an effort to advance that goal. In many respects the proposed definitions put forward by BIS and DDTC successfully clarify and streamline EAR and ITAR controls so as to facilitate understanding and accommodate the realities of technology and the international market.

In many important respects, however, the proposals move in the opposite direction. The straightforward and common approach to drafting regulations is to define terms consistent with their plain and common sense meaning and then apply clear rules to the defined terms.³ Many of the proposed definitions depart widely from the normal meaning of terms and encompass a variety of operational requirements. The distortion of definitions and conflation of definitions and rules underlie many of SIA’s reservations about the proposed rulemakings.

II. Proposed Definitions Appearing in Both the ITAR and EAR

A. Export (EAR §734.13; ITAR §120.17)

i. SIA Recommendation #1

The definition of “export” in EAR § 772.1 is a generally accurate definition that comports with the common sense meaning of the word and has stood the test of time. SIA believes it would be a mistake to eliminate this definition.

The ITAR definition of “export” should be aligned with the EAR definition of that term in EAR § 772.1.

Recommendation #1: BIS should retain the current definition of “export” in EAR § 772.1, and DDTC should add the following directly after ITAR § 120.17(a)(1): “(2) *The following activities are subject to these regulations in the same manner and with the same effect as exports: { then renumber (2) through (7) as (i) through (vii)}*.”⁴

² International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions, 80 Fed Reg. 31525 (Jun. 3, 2015) (“ITAR Harmonization Definitions”).

³ See “Drafting Legal Documents,” found at <http://www.archives.gov/federal-register/write/legal-docs/definitions.html> (“Do not define in a way that conflicts with ordinary or accepted usage. . . . Do not include a substantive rule within a definition.”)

⁴ SIA would support the definition of “export” in EAR § 772.1 to parallel the definition proposed in EAR § 734.13(a)(1).

ii. SIA Recommendation #2

The proposed regulation would create a new “definition” in EAR § 734.13(a). EAR § 734 sets forth the scope of the regulations and, among other things, “provides rules to determine whether items and articles are subject to the EAR.” The new “export” definitions set forth a series of rules in separate subsections that purport to define “exports,” “deemed exports,” certain “transfers,” “releases,” other “transfers,” and in the corresponding section of the ITAR, “making certain items available via a publicly available network.” There are several drawbacks to this approach to definitions.

Any regulatory scheme for exports should include “export” in the section setting forth relevant definitions. It is inherently confusing to include in the definition of “export” items that are not in fact exports, such as “deemed exports.” “Deemed export” should be defined in EAR § 772.1 and the rules governing deemed exports should be set forth explicitly in EAR § 734. This is a simpler and clearer way to proceed.

Recommendation #2: “Deemed export” should be defined in EAR § 772.1 and the rules governing deemed exports should be set forth explicitly in EAR § 734.

iii. SIA Recommendation #3

Failing to make a clear distinction between definitions and regulatory rules causes ambiguities. A major problem in this regard is the regulatory treatment governing the provision of theoretical access to controlled technology in the absence of actual access to that technology.

For example, if a building contains controlled items and a foreign national is given access to the building so as to be able to visually inspect the contents of the building, but the foreign national never in fact goes into the building for an inspection, did an export occur? More relevant to the semiconductor industry, if a foreign national information technology (IT) expert is given access to a database that contains controlled information, but the foreign national IT expert never in fact accesses the controlled information, that is, never views the controlled information, never downloads it and never comes in contact with it in any way, did an export occur?

Under the proposed definition of “export,” providing mere access would not appear to be a controlled event. “Release” is defined as inspections that “reveal” technology or source code to a foreign national or actions that constitute “oral or written exchanges” of technology with a foreign national.⁵ BIS explains that visual inspection “must actually reveal controlled technology or source code,” noting that this is a change from the more theoretical standard of the current regulations.⁶ Similarly, “exchanges” contemplate a give and take between the provider and the recipient. Mere theoretical access to technology or software does not rise to the level of an exchange of technology or software.

⁵ EAR Harmonization Definitions at 31,516.

⁶ *Id.* at 31,508.

At the same time, DDTC, and to a lesser extent BIS, indicate in the accompanying commentary, consistent with other actions in the regulations, that providing mere theoretical access to controlled items is a controlled activity. This is made explicit in connection with making technical data available via a public network such as the internet or the cloud.⁷ It is more opaque with respect to providing theoretical access to technical data or software within a private network to a particular foreign national.

Clarity on this point is important. Accordingly, BIS and DDTC should explicitly indicate whether providing theoretical access to technology, technical data or software to a foreign national constitutes an “export” in the absence of the foreign national ever actually accessing the technology, technical data or software.

Recommendation #3: BIS and DDTC should explicitly indicate whether providing theoretical access to technology, technical data or software to a foreign national constitutes an “export” in the absence of the foreign national ever actually accessing the technology, technical data or software.

iv. SIA Recommendation #4

Paragraph (a)(6) of the revised ITAR definition of “export” includes the phrase “regardless of whether such data has been or will be transferred.” That phrase does not appear in the EAR definition of “export” and should be removed. Only actual transfers of controlled technical data should constitute an export.

Recommendation #4: DDTC should remove the phrase “regardless of whether such data has been or will be transferred” from ITAR § 120.17(a)(6).

v. SIA Recommendation #5

If providing theoretical access to technology, technical data or software to a foreign national constitutes an “export” in the absence of the foreign national ever actually accessing the technology, technical data or software, then it would be important to distinguish between granting access via a public network (where the probability of actual access by a foreign national is substantial) and granting access via a secure, private network or database (where the probability of actual access by a foreign national is much less). New technologies make it possible to effectively monitor and detect such access.

SIA urges that any control placed on mere theoretical access include an explicit exception for access granted to company employees whose access is limited to technology, software or technical data housed within a secure company network. The exception would best be enumerated via a note to the “export” definition clarifying that providing theoretical access to a foreign national within a secure, private network is not an ‘export.’”

Recommendation #5: If BIS and DDTC determine that providing theoretical access to technology, technical data or software to a foreign national constitutes an

⁷ ITAR Harmonization Definitions at 31,529.

“export” in the absence of that foreign national ever actually accessing the technology, technical data or software , then BIS and DDTTC should include a note along the following lines in the definition of “export”:

Note: Making technology, technical data or software available to a foreign national via a private, secure network or database does not constitute an export or deemed export unless (i) the foreign national in fact accesses, downloads or otherwise reads or obtains possession of the technical data or (ii) the technical data is made available with the knowledge that the foreign national will access, download or otherwise read or obtain possession of the technical data.

vi. SIA Recommendation #6

BIS should publish a definition of “permanent residency” that is sufficiently broad to cover the variety of immigration statuses worldwide equating to U.S. lawful permanent residency (“green card”) status. Alternatively, BIS should change “permanent residency” to “legal residency” throughout the EAR.

Acquiring citizenship data for foreign national employees has become difficult due to the mobile nature of the modern workforce. In contrast, the United States and European countries, many Asian, African and Middle Eastern countries may not grant legal status to foreign nationals who have permanently settled in their country. Establishing residency in a third country without legal status equivalent to a U.S. ‘green card’ now is increasingly common.

In addition, requiring companies to collect proof of each foreign national employee’s nationality and permanent residency status may conflict with international privacy and anti-discrimination laws.

Immigration status often is not an accurate indicator of personal allegiances or national security sensitivity, and regulating deemed exports based on citizenship and permanent residency does not preclude willful violations of the EAR by individuals. Those foreign nationals who have chosen to emigrate and settle permanently in new countries with accordant long-term visa status should be afforded greater rights under the EAR with a broad, clear definition of “permanent” or “legal” residency beyond the confines of U.S. green card equivalency. By drawing a bright line between legal residency and temporary worker visa status, BIS and exporters would have fewer deemed export licenses to process, resulting in faster hiring of skilled workers and more efficient implementation of deemed export/reexport controls worldwide.

Recommendation #6: BIS either should publish a definition of “permanent residency” that is sufficient to cover the variety of immigration statuses worldwide which equate to U.S. permanent resident/green card holder status, or change “permanent residency” to “legal residency” throughout the EAR.

B. Technology (EAR § 772.1), Technical Data (ITAR §120.10), Required (EAR § 772.1; ITAR § 120.46) and Peculiarly Responsible (EAR § 772.1; ITAR § 120.46)

i. SIA Recommendation #7

DDTC has clarified the definition of “technical data” in the ITAR by adding a definition of “required.”⁸ “Required,” as applied to technical data, is said to mean “only that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.”

BIS should similarly clarify the EAR definition of “technology,” in order to give meaning to the first phrase in the EAR definition of “required” and align the two regulatory regimes on this point.

Recommendation #7: BIS should replace “necessary” with “required” in the EAR definition of “technology.”

ii. SIA Recommendation #8

BIS provides a definition of “peculiarly responsible” that offers a “catch and release” construct similar to that employed for the term “specially designed.”⁹

The ITAR does not define the words “peculiarly responsible,” presumably leaving the definition to the plain meaning of the words, but adds a note that technical data is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is otherwise used for the activities enumerated in ITAR § 120.10(a)(1).¹⁰

This additional construct for particularly responsible is a welcome change to the ITAR. Application of the proposed definition of “required” and the enhanced meaning of “peculiarly responsible” can be expected to have a substantive and limiting impact on the scope of items subject to the EAR and technical data subject to the ITAR.

The ITAR definition of “required” should apply to software as well as technical data, as is the case in the EAR. If it is used in the regulations in relation to software, the word “required” should have the same meaning as it does for technical data.

Recommendation #8: The ITAR definition of “required” should apply to software as well as technical data.

⁸ ITAR Harmonization Definitions at 31,534.

⁹ EAR Harmonization Definitions at 31,519.

¹⁰ ITAR Harmonization Definitions at 31,536.

iii. SIA Recommendation #9

The Note to paragraph (a)(1) of the EAR definition of “technology” is overly broad and should be clarified.

Recommendation #9: Note 1 to the EAR definition of “technology” should be modified as follows: “The modification of an existing item creates a new item, and technology *required* for the modification is ~~technical data for the development of~~ subject to the same controls as the new item.”

iv. SIA Comment

The proposed Note 1 to paragraph (a) under the definition of “required” in both the EAR and ITAR provides an essential confirmation of the application of the “peculiarly responsible” standard. Note 1 establishes that the peculiarly responsible standard can be applied to an item or defense article even if they have no specific technical parameters to describe the scope of what is controlled. In these cases, the peculiarly responsible standard will apply to the natural or plain meaning of the characteristics or functionality of the item or defense article, unless the characteristics or functionality are otherwise specified.

Application of the peculiarly responsible standard is illustrated with the example of a bomber, a defense article that is listed on the ITAR without any controlled technical parameters. According to Note 1, any technical data “peculiar to making” an aircraft a bomber would qualify as technical data “required” for a bomber and hence subject to the ITAR. The formulation “peculiar to the making” constitutes a useful elaboration of the peculiarly responsible standard.

To illustrate further, technical data for the targeting of a bomb sight in a bomber should qualify as technical data “peculiarly responsible” for the characteristics or functions of a bomber. In contrast, technical data for an elaborate cup holder for a bomber cockpit, that is, technical data unique to a bomber, would not qualify as ITAR technical data because the technical data for the cup holder is not peculiar to making an aircraft a bomber or peculiarly responsible for the controlled characteristics or functions of a bomber.

This Note 1 and its accompanying example are critical to industry’s understanding of and reliance on the peculiarly responsible standard. It is fully consistent with the common sense meaning of “peculiarly responsible.” It also reflects the long-standing meaning of the standard that has been applied by CoCom allies and currently applied by Wassenaar countries.

Lastly, Note 1 confirms that the “peculiarly responsible” standard is additive to the “catch and release” model of Note 3 to ITAR §120.46 and EAR § 772.1

v. SIA Recommendation #10

Note 2 to the paragraph (a) of the proposed ITAR definition of “required” and Note 2 to the proposed revised EAR definition of “required” both explain that the jurisdictional status of unclassified technical data or technology is the same as the jurisdictional status of the defense

article or item subject to the EAR to which it is directly related.¹¹ BIS and DDTC should clarify the meaning of this note by providing a clear and succinct definition of “directly related.” That definition of “directly related” should adhere closely to the new definition of “required” and thereby employ the new “peculiarly responsible” standard.

Recommendation #10: BIS and DDTC should clarify the meaning of Note 2 to the proposed revised EAR definition of “required” and Note 2 to paragraph (a) of the proposed ITAR definition of “required” by providing a clear and succinct definition of “directly related” that adheres closely to the new definition of “required” and thereby employs the new “peculiarly responsible” standard.

vi. SIA Recommendation #11

The introductory language of the EAR definition of “peculiarly responsible” references an “item,” while the subparagraph 3 of that definition references “information.” Given that the definition of “peculiarly responsible” may apply to hardware, software or technology, the use of “item” is more appropriate. BIS should replace “information” with “item” in subparagraph 3 of the “peculiarly responsible” definition.

Recommendation #11: BIS should replace “information” with “item” in subparagraph 3 of the “peculiarly responsible” definition.

vii. SIA Recommendation #12

Subparagraph 3 of the proposed definition of “peculiarly responsible” within the EAR and ITAR should apply to both hardware and software, and should utilize an alternative standard to “identical” for software.¹² An “identical” requirement for software is too confining. Instead, when dealing with tens, hundreds, or thousands of lines of software code, the standard employed in this “release” avenue should be “substantially similar to” rather than “identical.” It is common for various software of identical functionality to have minor and detailed differences that have no effect on performance levels, characteristics or functionality, i.e., differences that are insubstantial.

Recommendation #12: BIS and DDTC should revise the first sentence of subparagraph 3 of the “peculiarly responsible” definitions (within EAR § 772.1 and Note 3 to paragraph (a) of ITAR § 120.46, respectively) as follows:

(3) It is **hardware** identical to, **or is software substantially similar to,** an **item** used in or with a commodity or software that:

¹¹ EAR Harmonization Definition at 31,520; ITAR Harmonization Definitions at 31,536.

¹² EAR Harmonization Definitions at 31,520.

viii. SIA Recommendation #13

The proposed revised ITAR definition of “defense article” clearly establishes that software and technical data are separate and distinct categories of defense articles.¹³ That point should be made explicit within the ITAR definition of “technical data.”

Recommendation #13: DDTC should add the following at the end of paragraph (a)(1) of the ITAR definition of “technical data”:

“While electronic information meeting the preceding description may be technical data, “software” is not technical data.”

and should add the following to paragraph (b) of the definition: “(4) “Software.””

C. Transfer (in-country) (Proposed EAR § 734.16; Proposed ITAR § 120.51)

i. SIA Recommendation #14

The proposed EAR definition of “transfer” and the proposed ITAR definition of “retransfer” are expanded to include any change in end use within the same foreign country.¹⁴ This constitutes a fundamental alteration in the nature of export controls, is wholly inconsistent with the concept of transfer, and represents a substantial expansion of the extraterritorial reach of US controls contrary to principles of international law.

The proposal presents a variety of practical problems. Who is required to obtain permission from the US government to alter the use of an exported item? How and to what extent must a foreigner’s use be monitored? What constitutes a change in end use?

A transfer implies the presence of a transferor and a transferee, something not present in a change of use by the same end user. Creating the legal fiction of a transfer is confusing and unnecessary.

This new assertion of authority is sure to be met with resistance by foreign end users and pose a significant competitive impediment for US exporters. It is one thing for a foreign end user to agree as part of an export transaction to accept restrictions on further export or even transfer of the items received. However, it would be most unnatural to subject to US government authority a foreign end user’s own use of the items in his or her own country. In the vast majority of cases, the recipient will have paid for the items received, have clear title to and dominion over them and be acting in accordance with the applicable law of his or her country.

This extraterritorial expansion of US authority will also pose problems of law and jurisdiction for allied and friendly countries that make no such aggressive legal claims.

¹³ ITAR Harmonization Definitions at 31,526, 31,534.

¹⁴ EAR Harmonization Definitions at 31,516; ITAR Harmonization Definitions at 31,537.

In the past, concerns about end use were appropriately addressed within the particular facts and circumstances of an individual case. If US officials conclude that an end user is untrustworthy and poses a risk to US security and foreign policy through the use of a US export, they simply do not issue an export license. This process has worked well and should be continued.

No national security or foreign policy justification has been publicly provided for this change and the adverse consequences for US exporters have not been systematically analyzed for the public. These should be prerequisites before making the proposed changes in the EAR or the ITAR.

Recommendation #14: The proposed EAR definition of “transfer (in-country)” and the proposed ITAR definition of “retransfer” should omit any mention of end use.

D. Published and Public Domain (EAR § 734.7; ITAR § 120.11)

i. SIA Recommendation #15

SIA supports the proposed definition of “published,” and, in particular, paragraph 4 of the EAR proposed definition stating that “public dissemination . . . in any form . . . including posting on the Internet on sites available to the public” represents publishing of technology or software.¹⁵ SIA agrees with BIS that once technology or software has been publicly disseminated, they should no longer be controlled under any circumstances. Items that have been publicly disseminated are no longer controllable, and it is futile and counter-productive to try to impose controls with respect to such items.

In contrast, Note 1 to the proposed revised definition of “public domain” in the ITAR establishes a prohibition against exporting, reexporting, transferring or making available to the public ITAR technical data or software without government authorization if a person has knowledge that the technical data or software has been made publicly available without authorization.¹⁶ Lacking a public rationale or justification, this note runs directly counter to the EAR and common sense.

Furthermore, the revised ITAR definition of public domain also reflects the imposition of a prepublication approval requirement on public speech under the ITAR. Paragraph (b) of the revised definition explicitly sets forth the Department’s requirement of authorization to release information into the “public domain.” Prior to making available “technical data” or software subject to the ITAR, the U.S. government must approve the release through one of the following: (1) The Department; (2) the Department of Defense’s Office of Security Review; (3) a relevant U.S. government contracting authority with authority to allow the “technical data” or software

¹⁵ EAR Harmonization Definitions at 31,515.

¹⁶ ITAR Harmonization Definitions at 31,535.

to be made available to the public, if one exists; or (4) another U.S. government official with authority to allow the “technical data” or software to be made available to the public.¹⁷

The DDTC prepublication review requirement would operate as a prior restraint on free speech that applies to all would-be publishers of ITAR technical data, including to print and electronic news media outlets, engineering journals, public libraries, publishing houses, trade shows, and conference organizers. It also applies to persons who post information to electronic bulletin boards, company websites, and other online public forums.

In order both to enhance harmonization of the EAR and ITAR and adopt a more appropriate rule regarding technology or technical data in the public domain, DDTC should conform the ITAR to the EAR and dispense with any controls on technical data or software in the public domain.

Recommendation #15: DDTC should conform the ITAR definition of “public domain” to the EAR definition of “published” and dispense with any controls on technical data or software that have been publicly disseminated.

E. Activities That Are Not Exports, Reexports or Transfers (EAR § 734.18; Proposed ITAR § 120.52)

i. SIA Recommendation #16

Proposed new EAR § 734.18 and proposed new ITAR § 120.52 state that sending, taking or storing unclassified technology or software is not an “export,” “reexport” or “transfer” if the technology or software is

- (i) secured using end-to-end encryption,
- (ii) secured using cryptographic modules compliant with Federal Information Processing Standards Publication 140-2 or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications or “other similarly cryptographic means,” and
- (iii) not stored in a Country Group D:5 country.¹⁸

This is a very positive change which is supported by SIA. It is grounded in the modern reality of data protection and it will serve to enhance the secure transmission of data throughout the world.

At the same time, the precise nature of the improvement is unclear and uncertain, as several elements of the proposal are too constraining. In particular, the phrase “compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors” unnecessarily requires companies to adopt certain specific encryption algorithms. Instead, BIS

¹⁷ ITAR Harmonization Definitions at 31,528.

¹⁸ EAR Harmonization Definitions at 31,517; ITAR Harmonization Definitions at 31,537.

should require only that companies adopt encryption standards equivalent to and/or consistent with FIPS 140-2.

Recommendation #16: In new EAR § 734.18(a)(4)(iii) and new ITAR § 120.52(4)(iii), BIS and DDTC should replace “compliant with” with “equivalent to and/or consistent with”.

ii. SIA Recommendation #17

SIA supports BIS’s statement within proposed EAR § 734.18(a)(4)(iii) that “other similarly effective cryptographic means” are acceptable. DDTC should add this qualification to its companion proposal. In addition, DDTC too should require only that companies adopt encryption standards equivalent to and/or consistent with FIPS 140-2.

Recommendation #17: In new ITAR § 120.52(a)(4)(iii), DDTC should include that “other similarly effective cryptographic means” may be used to secure encrypted materials, and should replace “compliant with” with “equivalent to and/or consistent with”.

F. Development (EAR § 772.1 and General Technology Note; ITAR § 120.47)

i. SIA Recommendation #18

The inclusion of “serial” production within the definition of “development” in EAR § 772.1 and the General Technology Note and in ITAR § 120.47 is misguided and should be reversed. The term “serial production” no longer applies to much of the current manufacturing environment within the high technology sector. Companies may design, develop, manufacture and export “technology” for a single prototype or proof-of-concept device which may never be serially manufactured, but is still subject to the EAR. This is particularly true for items sent to custom foundries. Inclusion of “serial production,” rather than simply “production” within the definition of “development” makes that definition conflict with companies’ business model and customer demand. BIS and DDTC should remove “serial” from the “development” definition to ensure that definition focuses on refining the scope of “technology,” rather than restricting the scope based on the type of manufacturing.

Recommendation #18: BIS and DDTC should replace “serial production” with “production” in the definition of “development” in EAR § 772.1 and ITAR § 120.47.

III. Proposed ITAR Definitions

A. Software (ITAR §120.45(f))

i. SIA Recommendation #19

SIA applauds DDTC's clear distinction between software and technical data, with the former no longer being a subset of the latter.¹⁹ At the same time, greater clarity is needed as to the types of software controlled by the ITAR. Such clarification is best provided by a revised definition of "software."

"Software" is not among the ITAR terms for which a revised definition is proposed, but it should be. The current ITAR definition of "software" is both too narrow and internally inconsistent (insofar as it includes "software" within the definition of that term.)²⁰ A revised definition of software would be most helpful.

The EAR definition of "software" forms a good benchmark and provides a comprehensive regulatory meaning to that term which comports with the commonly-understood meaning of the term. Given the elegance of that EAR definition, and the U.S. government's stated goal of harmonization, DDTC should develop a revised ITAR definition of "software" that adheres to the EAR definition.

While inclusion of a comprehensive, all-encompassing description of "software" is warranted, it is also important that the new software definition make clear that only certain types of software are subject to ITAR control. Specifically, the new definition should clarify that only software peculiarly responsible for the controlled performance levels, characteristics or functions of a defense article is subject to ITAR control. Such narrowing of controls can be accomplished by insertion of the newly defined "required" into the software definition. That is, DDTC should make clear that only software "required" for a defense article is included within the ITAR definition of that term.

Recommendation #19: DDTC should revise the definition of "software" in the ITAR along the following lines:

A collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression and "required" for a defense article. For these purposes, "program" means a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer, and "microprogram" means a sequence of elementary instructions, maintained in a special storage, the execution of which is initiated by the introduction of its reference instruction into an instruction register.

¹⁹ ITAR Harmonization Definitions at 31,526.

²⁰ ITAR § 120.45(f).

B. Defense Service (ITAR §120.9)

DDTC should modify the proposed definition of “defense service” in several respects.

i. SIA Recommendation #20

Paragraph (a)(1) of the proposed revised definition of “defense service” stipulates that a defense service is provided only if a U.S. person “has knowledge of U.S.-origin technical data directly related to the defense article.”²¹ Accordingly, provision of a defense service requires the transfer of technical data directly related to a defense article. That point should be made explicit in paragraph (a)(1) of the new “defense service” definition.

Recommendation #20: DDTC should add the following at the end of paragraph (a)(1) of the revised “defense service” definition: “. . . and transfers to a foreign person that technical data directly related to a defense article.”

ii. SIA Recommendation #21

Paragraph (a)(2) of the proposed revised definition of “defense service” classifies as a defense service the furnishing of assistance in the “integration of a defense article with any other item.” The Note to paragraph (a)(2) goes on to state that “Integration includes the introduction of software to enable operation of a defense article...”

This proposed definition of software “integration” is so broad and ambiguous as to include almost any activity involving software. That is, any activity associated with introducing or facilitating the introduction of software into a defense article could be captured by the proposed definition of “integration.”

In addition, and contrary to a statement in the same Note, there does not appear to be any meaningful distinction for software between “integration” and “installation.” While “installation” is described to exclude the use of technical data, “integration” is defined to include “the introduction of software” regardless of whether technical data is used to do so. On its face, “introduction” is indifferent to the use of technical data, thereby failing for software to provide a basis to distinguish “integration” from “installation.”

Defining integration to include any “introduction of software to enable operation” eliminates the focus on the relationship of the software to the defense article. The software need not be “required,” “peculiarly responsible,” or “specially designed” for the defense article, nor even contribute to the controlled performance levels, characteristics or functions of the defense article for it to be deemed “integrated” into the defense article. Such a definition of “integration” is contrary to the plain meaning of the word and, again, eliminates any distinction between “integration” and “installation” in the case of software.

DDTC should modify the definition of “integration” provided in the Note to paragraph (a)(2) to include only introduction of software “required” for a defense article – i.e., software peculiarly responsible for achieving or exceeding the controlled performance levels,

²¹ ITAR Harmonization Definitions at 31,534.

characteristics or functions of the defense article.²² The introduction of software not peculiarly responsible for the controlled characteristics of the defense article should be explicitly included in the definition of “installation.” By doing so DDTC would give meaning to the distinction between “integration” and “installation” for software and would appropriately classify as a “defense service” only the introduction of software that meaningfully contributes to the controlled characteristics of a defense article.

In addition, DDTC should make clear that software “integration” necessarily involves both the knowledge of U.S.-origin technical data and the use of such technical data. In the Note to paragraph (a), DDTC establishes that servicing of an item integrated into a defense article without the use of technical data is not a defense service.²³ DDTC should adopt the same position vis a vis software. That is, if DDTC insists on covering “integration” as a defense service, then it should clarify that software introduced or installed into a defense article without the use of technical data is not “integration” of the software. There is no reason to distinguish between hardware and software in that regard.

Finally, DDTC should make clear that “integration” does not cover the mere provision or transfer of software, and that instead software “integration” requires actual engagement with a customer in such a way that the software and defense article are blended and indivisible. In this context, software “integration” should occur only when provision of software includes activity specifically enhancing the controlled performance levels, characteristics or functions of a defense article. “Integration” should exclude any activity that relates solely to fit.

Recommendation #21: DDTC should revise the Note to paragraph (a)(2) of the “defense service” definition as follows:

“Integration” means any engineering analysis (see § 125.4(c)(5) of this subchapter) needed to unite a defense article and one or more items. Integration includes the introduction of software required to enable operation of for a defense article if such introduction involves both the knowledge of U.S.-origin technical data and the use of such technical data, and the determination during the design process of where an item will be installed (e.g., integration of a civil engine into a destroyer that requires changes or modifications to the destroyer in order for the civil engine to operate properly; not plug and play). Software integration occurs only if the provider of the software engages with the customer in such a way as to render the software and defense article blended and indivisible and involves activity specifically enhancing the controlled performance levels, characteristics or functions of the defense article. Software integration does not include modification to software to achieve the fit of the software with respect to the defense article. Integration is distinct from “installation.” “Installation” means the act of putting an item including software in its predetermined place without the use of technical data or any modification to the defense

²² Please see the discussion of the “required” definition above.

²³ ITAR Harmonization Definitions at 31,534.

article involved, other than to accommodate the fit of the item with the defense article (e.g., installing a dashboard radio into a military vehicle where no modifications (other than to accommodate the fit of the item) are made to the vehicle, and there is no use of technical data.). Introduction of software into a defense article represents installation, rather than integration, if the only modifications made to the software or defense article are related to fit. The “fit” of an item is defined by its ability to physically interface or connect with or become an integral part of another item.

iii. SIA Recommendation #22

Among the activities deemed not be a “defense service” in the Note to paragraph (a) is “[T]he furnishing of assistance by a foreign person not in the United States.” This example is straightforward and unqualified. Read in context, its meaning is clear.

In its discussion of the proposed definition of “defense service,” however, DDTC notes:

the furnishing of a type of assistance described by the definition of a “defense service” is not an activity within the Department’s jurisdiction when it is provided by a foreign person outside the United States to another foreign person outside the United States on a foreign “defense article” using foreign-origin “technical data.”²⁴

The latter two conditions noted by DDTC – that the service be on a foreign defense article and use foreign-origin technical data -- do not appear in the proposed regulatory language (*i.e.*, in paragraph 6 of the proposed Note to paragraph (a)) and are not apparent from the language itself.

As a result, there appears to be a significant disconnect between the plain meaning of the language in paragraph 6 of the proposed Note to paragraph (a) and the manner in which DDTC intends to interpret that language. Such ambiguity is counterproductive and creates confusion for exporters.

There is no justification for limiting this exclusion to assistance employing foreign-origin “technical data.” Determining whether technical data is of foreign origin often is extremely challenging and subjective, especially when the technical data at issue was generated by a company with both U.S. and foreign operations. In addition, the distinction between foreign-origin technical data and U.S.-origin technical data is inappropriate in this context. Assistance provided by a foreign person located in a foreign country to another foreign person located in a foreign country should not be designated as a “defense service” regardless of the type of technical data employed in the assistance.

In order to avoid unnecessary ambiguity and clarify the bounds of ITAR jurisdiction, DDTC should explicitly state in the Note to paragraph (a) that furnishing of assistance by a foreign person not in the United States is not a “defense service” regardless of the type of assistance provided or the type of technical data employed in doing so.

²⁴ ITAR Harmonization Definitions at 31,530. (emphasis added.)

Recommendation #22: DDTC should explicitly state in item 6 of the Note to paragraph (a) of the “defense service” definition that furnishing of assistance by a foreign person not in the United States is not a “defense service” regardless of the type of assistance provided or the type of technical data employed in doing so.

iv. SIA Recommendation #23

In item 3 of the Note to paragraph (a) of the defense service definition, DDTC notes that servicing of an item subject to the EAR that has been incorporated into a defense article is not a defense service.²⁵ DDTC should clarify that servicing may include introduction of software updates, patches and bug fixes.

Recommendation #23: DDTC should include the following at the end of item 3 of the Note to paragraph (a) of the “defense service” definition:

In the case of EAR-controlled software incorporated into a defense article, “servicing” may include introduction of software updates, patches and bug fixes.

v. SIA Recommendation #24

In conjunction with the software-related revision discussion above, DDTC also should explicitly note that provision of commercial software without the transfer of technical data is not a defense service.

Recommendation #24: DDTC should add the following at the end of the Note to paragraph (a) of the “defense service” definition:

10. The introduction of commercial software into a defense article without the transfer of technical data directly related to the defense article.

C. Production (New ITAR §120.48)

i. SIA Recommendation #25

The proposed ITAR definition of “production” inappropriately includes integration. The scope of integration is far too elastic and amorphous to be included in production. Instead, integration is an activity that occurs between items that already have been produced.

Recommendation #25: DDTC should remove “integration” from the ITAR definition of “production.”

ii. SIA Recommendation #26

The term “serial production” no longer applies to much of the current technology/manufacturing environment. Production exists at any level of volume, and there

²⁵ ITAR Harmonization Definitions at 31,534.

should not be any distinction between production of one hundred items or hundred thousand items. DDTC should remove the discussion of “serial production” from the “production” definition to ensure that definition captures the full range of production.

Recommendation #26: DDTC should delete the discussion of “serial production” from the ITAR definition of “production.”

D. Reexport

i. SIA Recommendation #27

Paragraph (a)(4) of the revised ITAR definition of “reexport” includes the phrase “regardless of whether such data has been or will be transferred.” That phrase does not appear in the EAR definition of “export” and should be removed. Only actual transfers of controlled technical data should constitute a reexport.

Recommendation #27: DDTC should remove the phrase “regardless of whether such data has been or will be transferred” from ITAR § 120.19(a)(4).

E. Technical Data that Arises During or Results from Fundamental Research (New ITAR § 120.49)

SIA supports the inclusion of this definition within the ITAR. Nevertheless, both Notes to paragraph (a) of the proposed definition are in need of revision.

i. SIA Recommendation #28

DDTC should revise Note 1 to paragraph (a) of the definition to remove any mention of equipment or software. Neither equipment nor software is or can be technical data, so neither should be included in this definition pertaining to technical data.

Recommendation #28: DDTC should revise Note 1 to paragraph (a) of new ITAR § 120.49 to remove any mention of equipment or software.

ii. SIA Recommendation #29

As currently drafted, Note 2 to paragraph (a) of the definition could be interpreted to mean that the designation of technical data as being subject to the ITAR is irrevocable. Such an irrevocable ITAR designation would be wholly inappropriate, as unclassified data developed by a private researcher, institution or company should be removed from ITAR jurisdiction whenever it no longer qualifies for such jurisdiction.

Recommendation #29: DDTC should add the following at the end of Note 2 to paragraph (a) in new ITAR § 120.49: “Such technical data shall no longer be subject to ITAR jurisdiction if it otherwise becomes exempt from ITAR jurisdiction.”

iii. SIA Comment

SIA supports the clarification of the “fundamental research” definition. Industrial business units engaged in research and development collaborate on publications for the wider scientific and technical community in addition to their work on proprietary research. By using this proposed definition, entities will be able to implement concrete process changes to track fundamental research activities for compliance to determine if and when a research project falls under the scope of the EAR per Note 2 to paragraph (a).

* * * * *

SIA appreciates the opportunity to comment on the Proposed Revisions and looks forward to continuing its cooperation with the U.S. Government on export control reform. Please feel free to contact the undersigned or Joe Pasetti, Director of Government Affairs at SIA, if you have questions regarding these comments.



Cynthia Johnson
Co-Chair, SIA Export Control Committee



Mario R. Palacios
Co-Chair, SIA Export Control Committee

August 3, 2015

U.S. Department of Commerce
Bureau of Industry and Security
Regulatory Policy Division
Room 2099B
14th Street and Pennsylvania Ave. NW
Washington, D.C. 20230

Sent via email to: publiccomments@bis.doc.gov

Re: RIN 0694–AG32 - Revisions to Definitions in the Export Administration Regulations

Dear Sir/Madam:

Google welcomes the opportunity to comment on the proposed rule regarding the definition of various terms in the Export Administration Regulations (“EAR”). On June 3, 2015, the Commerce Department’s Bureau of Industry and Security (“BIS”) published a proposed rule in the Federal Register entitled Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32). (See 80 Fed. Reg. 31505.) We provide comments on the following definitions.

Definition of “Peculiarly Responsible”

In the Federal Register notice of this proposed rule, BIS asked whether the proposed definition of “peculiarly responsible” effectively explains how items may be “required” for particular functions. It does not. The proposed definition reaches too far and would control too much information (i.e. “technology”). In particular, the “release” portion of the “catch and release” process laid out in the proposed definition will lead to too many absurd results. In the overwhelming majority of analyses, the illustration of technologies “A,” “B,” “C,” “D,” and “E” in the existing definition of “required” is sufficient to distinguish technologies that are peculiarly responsible (and thus controlled) from those that are not.

In the term “peculiarly responsible,” it is significant that “responsible” is modified by the word “peculiarly,” which denotes a special, causal relationship with the thing that is being controlled. The proposed definition of “peculiarly responsible” effectively removes “peculiarly” from the equation and controls a wider swath of “technology” than is warranted.

We will provide examples where the proposed definition of “peculiarly responsible” leads to odd and undesirable results. These examples are oversimplified to some degree, but they are intended to be simple for the sake of illustration and to avoid discussing any specific examples that could reveal Google confidential information. We also comment on the relationship between the proposed definition and the General Technology Note, and we offer recommendations regarding the proposed definition.

A. Example 1: Heat Sink Design “Technology”

Assume that a U.S. company called “Heats Inc.” produces heat sinks for a variety of computer manufacturers. Suppose that all but one of Heats Inc.’s customers make mass-market computers classified under ECCN 4A994, and they purchase Heats Inc.’s straight-fin heat sinks having a length and width of one inch. The 1” x 1” heat sink and its design “technology” would both be classified under EAR99. Say that Heats Inc.’s other customer, “HPC,” manufactures computers classified under ECCN 4A003.b and purchases straight-fin heat sinks with a length and width of two inches. Heats Inc. only sells 2” x 2” heat sinks to HPC, has no intent to sell or market them to other computer manufacturers, designed the larger heat sink at HPC’s specific request, and learned during the course of business discussions that HPC’s computers are classified under 4A003.b. Assume that Heats Inc. is the only heat sink manufacturer in the world producing straight-fin heat sinks measuring two inches by two inches. Further assume that the only difference in the design of the two types of heat sinks is in the length and width dimensions.

Now let us determine the ECCN of the design technology for the 2” by 2” heat sink using the “catch and release” process in the proposed definition of “peculiarly responsible.”

The “catch” portion of the “peculiarly responsible” definition applies to the design of the 2”x 2” heat sink. Under the proposed definition, an item is:

“peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR....

Here, the heat sink is used in a 4A003.b computer, and the design information (i.e., “technology”) for the heat sink is used in the creation (i.e., “development” or “production”) of a 4A003.b computer. Therefore, its design information falls within the scope of the “peculiarly responsible” definition.

However, the “release” portions of the “peculiarly responsible” definition do not apply to the design “technology” of the heat sink for the 4A003.b computer. Under the proposed definition,

“technology” meeting the first part of the definition is controlled under the applicable ECCN (in this example, 4E001) unless:

- (1) The Department of Commerce has determined otherwise in a commodity classification determination;
- (2) [Reserved];
- (3) It is identical to information used in or with a commodity or software that: (i) Is or was in production (i.e., not in development); and (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
- (4) It was or is being developed with “knowledge” that it would be for use in or with commodities or software: (i) Described in an ECCN; and (ii) Also commodities or software either not enumerated on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
- (5) It was or is being developed for use in or with general purpose commodities or software, i.e., with no “knowledge” that it would be for use in or with a particular commodity or type of commodity; or
- (6) It was or is being developed with “knowledge” that it would be for use in or with commodities or software described: (i) In an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) Exclusively for use in or with EAR99 commodities or software.

Assume that number (1) does not apply because no commodity classification determination has been sought by Heats Inc. for its 2” x 2” heat sink design “technology.”

Number (3) would not apply to the 2” x 2” heat sink design because its design is not *identical* to the EAR99 design of the 1” x 1” heat sink. The former is an inch greater in length and width. The design information (i.e., “development” or “production” “technology”) for the two types of heat sinks would reflect this difference in physical dimensions even if everything else about them is the same.

Number (4) would not apply to the 2” x 2” heat sink design because the larger heat sink is only being used on 4A003.b computers and was not developed with an intent for or knowledge of use on 4A994 computers.

Numbers (5) and (6) would not apply to the 2” x 2” heat sink design because Heats Inc. created the larger heat sink at HPC’s request, knows that HPC uses them for 4A003.b computers, and has never intended to sell the larger heat sinks on the general computing market.

Therefore, under the proposed definition of “peculiarly responsible,” Heats Inc. would be compelled to classify the design “technology” of its 2” x 2” heat sink under 4E001.a. This bizarre and unexpected result is not reached under the EAR as it exists today.

The design “technology” of the 2” x 2” heat sink would not be controlled under the current definition of the term “required.” 4A003.b applies to computers whose “Adjusted Peak Performance” exceeds 8.0 weighted TeraFLOPS (“WT”), as calculated by a formula provided in Category 4 of the Commerce Control List (CCL). The WT value of a computer is a function of its processors’ architectures (such as 64-bit floating point operations) and speed (i.e., frequency), as well as the aggregation of the computer’s processors as calculated under the WT formula in Category 4 of the CCL. Today, an exporter can satisfactorily resolve the heat sink design technology classification question under the existing definition of “required,” which controls:

... only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions.... For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note.

In the Heats Inc. hypothetical, the heat sink in the 4A003.b computer has no impact on the latter’s WT calculation. Nothing about the heat sink can alter the variables that contribute to a computer’s WT value. The heat sink cannot, for instance, make the computer run another 64-bit floating point operation; it has no bearing on integrated circuit architecture. The heat sink design cannot make the computer’s microprocessors run at a higher frequency than the processor’s silicon will naturally support. The presence of a heat sink in a computer does not result in the aggregation of multiple microprocessors under Category 4’s WT formula. The heat sink thus has no causal relationship whatsoever with the variables that determine computer’s WT value; i.e., the heat sink has no ability to make a computer achieve or exceed its controlled performance level of 8.0 WT. Therefore, the heat sink is not peculiarly responsible for HPC’s computers achieving or exceeding that performance threshold, and the design of the 2” x 2” heat sink would thus not be controlled under 4E001 today. Rather, the heat sink design would be classified as EAR99 “technology,” which is a reasonable, common-sense outcome.

B. Example 2: Motherboard Design “Technology”

Consider another example involving two different motherboard manufacturers, Mobo One and Mobo Two, and two microprocessor manufacturers, CPU-A and CPU-B. Mobo One has

designed a four-socket motherboard for a computer using four microprocessors from CPU-A, and the resulting system falls below 8.0 WT. Assume that Mobo Two has designed a four-socket motherboard for a computer using four microprocessors from CPU-B, and with CPU-B's superior microprocessors, this system reaches 8.1 WT and is thus classified under 4A003.b.

Here, Mobo Two's motherboard design "technology" is "caught" under the proposed definition of "peculiarly responsible" because the board design "technology" is "used in or for use in" the "development" or "production" of a 4A003.b computer.

It is not difficult to imagine a set of business circumstances that fail all of the "release" provisions in the proposed definition of "peculiarly responsible." Maybe Mobo Two is designing the motherboard only for this specific model of processor from CPU-B such that this board design is not completely identical to a board already in mass production for computers classified under 4A994 (even if those differences are trivial in nature, such as the location of a USB port or placement of a single resistor). Maybe the customer's delivery schedule requirements make it impractical for Mobo Two to obtain a commodity classification determination prior to designing and manufacturing the motherboard that uses CPU-B's processors. In this example, applying the proposed definition of "peculiarly responsible" would produce a "catch" but not a "release," making the board design constitute 4E001 "technology," which is an improper result because the motherboard has no ability to modify the technical parameters that can make a computer fall within the scope of 4A003.b. I.e., motherboard design is orthogonal to the WT value of a computer. For example, a motherboard cannot perform a 64-bit floating point operation. A motherboard cannot enable a microprocessor to run at a higher frequency than the silicon itself will allow. The board design information (i.e., "technology") does not have any unique properties "for achieving or exceeding the controlled performance levels, characteristics or functions" of a 4A003 computer. In this example, it is simply a coincidence that CPU-B's microprocessors drive the system above the 8.0 WT control threshold. The motherboard could theoretically have been tweaked to accommodate another company's lower-performing microprocessors. Business circumstances simply did not lead to that fate. Therefore, there is not a good reason to treat information about Mobo Two's board design as controlled 4E001 "technology."

Many similar examples could be found for a wide variety of technologies.

C. The Proposed Definition Is Inconsistent With The General Technology Note

Exclusion (4) in the proposed definition of "peculiarly responsible" is inconsistent with the text of the General Technology Note. In Supplement No. 2 to Part 744 of the EAR, the General Technology Note states that:

"Technology" "required" for the "development", "production", or "use" of a controlled product remains controlled **even when applicable to a product controlled at a lower level**. (Emphasis added.)

However, exclusion (4) in the proposed definition of "peculiarly responsible" would not control "technology" if:

It was or is being developed with "knowledge" that it would be for use in or with commodities or software: (i) Described in an ECCN; and (ii) Also commodities or software either not enumerated on the CCL or the USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons....

If BIS adopts its proposed definition of "peculiarly responsible," we encourage BIS to resolve this inconsistency, which would likely be a source of confusion for exporters. However, Google recommends simply not adopting a specific definition for the term "peculiarly responsible" and continuing to use the existing definition of "required," which provides adequate guidance to satisfactorily resolve the vast majority of classification decisions and causes no conflict with the General Technology Note.

D. Recommendations For Alternative Definition

Google's preference is for BIS not to define the term "peculiarly responsible." Any benefits it would provide in terms of clarity are outweighed by detriments it would cause by controlling some technologies unnecessarily. However, if BIS insists on creating a specific definition for the term, then it could improve the definition by the following:

1. Amend the third exclusion to read: "It is identical or substantially similar to information used in or with a commodity or software that is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons." Please note that this recommendation also removes the proposed definition's clause "Is or was in production (*i.e.*, not in development)." If a piece of information is unrelated to the technical reasons for an end-item's control, it should not matter that the information also relates to an item manufactured at a sufficient volume to constitute "production" as opposed to "development." It is unclear how the distinction between "development" and "production" provides a reasonable basis for potentially controlling information that is orthogonal to the reason(s) for an item on the CCL being controlled.
2. Otherwise clarify that information (*i.e.*, "technology") is not "peculiarly responsible" and thus not controlled if it does not have any causal impact on the technical performance levels or characteristics that the CCL uses to capture an end-item.

Definition of “Required”

If BIS establishes a formal definition of the term “peculiarly responsible,” then it should place this term in quotation marks when it appears in the definition of the word “required” so that exporters will know that they should cross-reference the definition of “peculiarly responsible.” Otherwise, readers of “required” will not necessarily be aware that they need to consult both definitions in order to resolve their classification issues.

Additionally, if BIS creates a formal definition of the term “peculiarly responsible” and does not incorporate any of the suggestions that we have recommended above for that term, then it should eliminate from the definition of “required” the illustration regarding technologies “A,” “B,” “C,” “D,” and “E” for a widget operating at or above 400 MHz. This illustration within the definition of “required” does not contain sufficient factual detail to establish clearly that technologies A through C are not “peculiarly responsible” under the “catch and release” analysis proposed for that term, especially the “releases” in numbers (1) through (6) of the proposed “peculiarly responsible” definition. This inconsistency between proposed definition of “peculiarly responsible” and the existing example within the term “required” indicates a deficiency in the former. If the proposed “peculiarly responsible” term is not rejected -- or at least significantly altered, the illustration is incomplete at best, misleading at worst, and should be removed from the definition of “required.”

Definition of “Technology”

Proposed § 772.1 of the EAR includes in its definition of “technology”:

(a)(5) Information, such as decryption keys, network access codes, or passwords that would allow access to other “technology” in clear text or “software.”

If a decryption key (or other means of accessing materials in clear text) is treated as “technology,” making the key publicly available would remove the key from the scope of the EAR. If the key is no longer subject to the EAR, what is the consequence, if any, to the classification of the material that it decrypts? E.g., would that encrypted material also become publicly available and removed from the scope of the EAR (regardless of whether the clear text of the encrypted material has directly been made publicly available)?

Definition of “Export”

A. BIS should delete the term “or permit” from proposed § 734.13(a)(6).

Proposed § 734.13(a)(6) defines as an export:

Releasing or transferring decryption keys, network access codes, passwords, software, or other data with “knowledge” that such provision will cause **or permit** the transfer of other technology or software in clear text to a foreign national.” (Emphasis added.)

Now consider the following key or password:

E2ArxmM6kKxPzSADzcQK

It is a logical truth -- and, therefore, we have knowledge -- that this string of numbers and letters permits any person, including foreign nationals, to access in clear text any technology or software that has been protected by the code “E2ArxmM6kKxPzSADzcQK.” However, we have no idea whether any technology or software in the world actually exists that is protected by this random string of numbers and letters. Furthermore, we have no idea what ECCNs may apply to such technology or software. By their very nature, decryption keys, network access codes, passwords, and the like permit access to their associated protected material. Any transfer of decryption keys, network access codes, passwords, etc. would necessarily result in knowing that access to the protected materials has been permitted (i.e., theoretically allowed).

We are also concerned about the fundamental fairness of BIS creating liability for merely permitting a technology or software transfer if no actual (or high probability of an actual) violation occurs. For instance, consider a situation where a simple administrative error takes place and a foreign person is temporarily given access to a system that would theoretically permit this person to access controlled technology or software. As a matter of fairness and as a measure of actual harm, it is materially different comparing a situation where this foreign person were actually to view or download controlled technology or software before the administrative error was detected with another situation where the foreign person merely had access for a period of time but never actually viewed or downloaded controlled material. If no transfer of technology or software takes place, an “export” should not be established under the EAR.

Accordingly, BIS should delete the term "or permit" from proposed § 734.13(a)(6).

B. BIS should add the modified "knowledge" provisions of proposed § 734.13(a)(6) to the deemed export rule in proposed § 734.13(a)(2).

Proposed § 734.13.(a)(6) defines as an export:

Releasing or transferring decryption keys, network access codes, passwords, software, or other data with “knowledge” that such provision will cause or permit the transfer of other technology or software in clear text to a foreign national.

Proposed § 734.13.(a)(2) defines as a deemed export:

Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”).

The definition of "technology" in proposed § 772.1(a)(5) includes "[i]nformation, such as decryption keys, network access codes, or passwords that would allow access to other 'technology' in clear text or 'software.'" Therefore, any transfer of a decryption key, etc. to a foreign national in the United States would be treated as a deemed export.

We request that BIS make § 734.13(a)(2) consistent with (a)(6) and include an equivalent "knowledge" requirement. The rationale for including a "knowledge" requirement in (a)(6) -- and limiting it to "knowledge" of actual, not theoretical, access to controlled materials -- is identical to requiring "knowledge" of actual, not theoretical, access to controlled "technology" or "source code" for purposes of a deemed export.

Accordingly, § 734.13(a)(2) should be changed to read:

Releasing or otherwise transferring “technology” or “source code” (but not “object code”) to a foreign national in the United States (a “deemed export”). Releasing or transferring decryption keys, network access codes, passwords, software, or other data is a deemed export when made with “knowledge” that such provision will cause the transfer of other technology or source code in clear text to a foreign national.

Definition of Reexport & Deemed Reexport

The comments and recommendations above regarding "export" and "deemed export" also apply to the proposed definitions of "reexport" and "deemed reexport."

Activities That Are Not Exports, Reexports, Releases, Retransfers, or Transfers

Proposed § 734.18(a) lists a number of activities that are not treated as exports, reexports, or transfers for purposes of the EAR. Proposed § 734.18(a)(4) includes sending, taking, or storing “technology” or “software” that is, among other things, secured using 'end-to-end encryption.' Proposed § 734.18(b) states that "'end-to-end encryption' means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider."

Although the creation of this exclusion from the scope of the EAR is useful, it is unlikely to be used widely. End-to-end encryption as described by the proposed regulation is relatively uncommon in cloud computing environments. Where it exists, it is used most frequently in cloud

storage services. However, it does not even represent the majority of usage in cloud storage environments. Outside of cloud storage, end-to-end encryption is found even less frequently in the provision of cloud-based services. Introducing end-to-end encryption to cloud services often results in the loss of too many useful features desired by cloud computing customers. For instance, in cloud-based email systems, it would result in the loss of features like search, spell check, and spam detection. Accordingly, the overwhelming majority of cloud computing providers, users, and uses will fall outside the scope of proposed § 734.18. The proposed regulation does not make clear how it intends to treat cloud transactions in environments that do not use end-to-end encryption. Based on conversations with BIS, however, our understanding is that those transactions would be governed by the existing advisory opinions that BIS has issued on cloud computing, which industry has relied upon for the last several years.

Thank you for your consideration. Please do not hesitate to contact us via email (neilmartin@google.com) or phone (650-253-1816) with any questions or comments regarding this submission.

Respectfully,

Neil Martin

Export Compliance Counsel
Google Inc.



August 3, 2015

Submitted Via E-Mail (DDTCTPublicComments@state.gov) & (publiccomments@bis.doc.gov)

Mr. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C.

Ms. Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C.

Re: Comments on Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) (RIN 1400-AD70 and RIN 0694-AG32)

Lockheed Martin Corporation (Lockheed Martin) is pleased to submit the following comments in response to the Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) (See 80 Fed. Reg. 106 at 31525 and 80 Fed. Reg. 106 at 31505) published in the Federal Register on June 3, 2015.

Lockheed Martin commends the Departments of State and Commerce for the continuing effort to harmonize the definitions and terms used in the ITAR and EAR. This will help to prevent conflicting regulatory guidance and ease compliance efforts. It is critical, however, that such efforts do not inadvertently expand controls on common business practices or increase the complexity of the U.S. export control regime. In the effort to have agreement between the ITAR and EAR, we also encourage the Departments to identify ways in which licensing, reporting, and recordkeeping requirements should be reduced. While harmonized definitions will provide needed clarity, it is also imperative to streamline and facilitate the export licensing process to achieve the stated goals of the President's Export Control Reform (ECR) initiative, including focusing controls on the most sensitive transactions and technologies.

I. ITAR §120.10: Technical Data / EAR §772.1: Technology

Installation: As proposed, §120.10(a)(1) controls "installation" as technical data for a defense article. This is inconsistent with the Note to paragraph (a)(2) in the proposed Section §120.9

Defense Service, which explicitly notes that “installation” is performed without the use of technical data. Accordingly, the definition of technical data should exclude “installation” to ensure consistency and clarity.

Recommendation: Remove the term “installation” in the definition of technical data.

Information Controls: §120.10 (a)(5) controls decryption keys, network access codes, or passwords that would allow access to other technical data. Yet, this information is not controlled under the ITAR. Instead, the ITAR appropriately controls the technical data that is to be accessed and does not need to control the means for access. There are several practical reasons to limit controls to the technical data and not the passwords: first, it unnecessarily complicates providing such information to authorized individuals; and second, it could inadvertently control common terms used as passwords in other documents.

Recommendation: Delete (a)(5) from §120.10.

Non-Proprietary Controls: The proposed language of §120.10(b)(1) excludes “non-proprietary” information. By implication, the definition would control “proprietary” information as “Technical Data.” There are situations where some information in a general system description is controlled by the author for confidentiality and circulation reasons. In this context, all descriptions related to a defense article that contain proprietary information in a general system description would be controlled as Technical Data under the ITAR. This would greatly expand the definition of Technical Data.

Recommendation: Remove “non-proprietary” from §120.10(b)(1).

Removal of “Software”: Removing “software” from the definition of “technical data” is appropriate. However, the change has significant implications for existing authorizations and future compliance responsibilities, as the ITAR includes hundreds of references to Technical Data. It is imperative that the removal of “software” does not create gaps in a USML category or inadvertently remove current authorizations included in ITAR exemptions.

Recommendation: Lockheed Martin recommends the Department of State draft a separate proposed rule to provide a clear definition of “software” and an opportunity for the public to comment on where changes are warranted in the ITAR to address the removal of “software” from the definition of “technical data.” In addition, we recommend the Department of State provide guidance regarding the completion of license applications to account for the current two options for the “commodity” block in a license application (i.e., DSP-5): “Hardware” or “Technical Data”. For cases that include limited defense services, the USG has the capability to authorize the case based on §124.1(a), which defines the standard for approval. Without a modification to the existing forms or a similar provision in the ITAR, the authority and process to issue licenses for software will be unclear.

Technology: The use of the term “technology” to describe information “...result[ing] from...” fundamental research in §734.8 appears to contradict the proposed note that “information that is not ‘technology’ as defined in the EAR is per se not subject to the EAR.”

Recommendation: We recommend replacing the term “technology” in §734.8(a) with the term “information”.

II. ITAR §120.11: Public Domain

Ascertaining the Source of Public Information: Once information is in the public domain, it may be impractical, if not impossible, to determine whether technical data has been approved for such release. Paragraph §120.11(b) effectively prevents any U.S. person from assuming that publically available information is not controlled under the ITAR without making separate formal inquiries to the U.S. Government.

For example, Company A presents an article intended for publication in an open source magazine to Department of Defense, Office of Security Review prior to sending the article to the publication. The article contains some information that is Technical Data. The Department of Defense, Office of Security Review approves the article for release with revision. Utilizing 125.4(b)(13), Company A enters the information into the Public Domain. Any Person may access the information in the Public Domain, except that no one other than Company A knows that the information in the article is by definition in the public domain. This not only imposes a significant compliance burden on U.S. companies that must determine whether an appropriate review was conducted, but it also may provide commercial advantages to specific companies that have knowledge of that review and can more efficiently utilize the data in the public domain.

Recommendation: The U.S. Government must revisit the “knowledge” standard with regard to information in the public domain to prevent a cumbersome and impractical review requirement for information already in the public domain.

III. ITAR §120.17 / EAR §734.13: Export

Deemed Exports: The proposed revision to the definition in Sec. 120.17(b) maintains two different “deemed export” license requirements for foreign nationals. The Department of Commerce reviews deemed export applications based on a foreign national’s most recent country of citizenship or permanent residency, while the Department of State reviews deemed export based on all countries in which the foreign person has held citizenship or holds permanent residency. The intent of ECR is to harmonize such licensing requirements. Maintaining two standards is contrary to this objective and complicates industry compliance efforts, particularly if a foreign national is the recipient of both ITAR and EAR controlled items.

Recommendation: Lockheed Martin recommends reconciling the two definitions by removing “... and all countries in which the foreign person has held citizenship” and revising 120.17(b) as follows:

“(b) Any release in the United States of Technical Data or software to a Foreign Person is a deemed export to the Foreign Person’s most recent country of citizenship or permanent residency.”

Exports of Spacecraft: The proposed definition for “export” appears to exclude the export of spacecraft that are not destined to a D:5 country and do not meet the STA license exception criterion. This could create a scenario where a U.S. person does not require export authority to transfer registration or ownership of a spacecraft to a customer from an STA country if the spacecraft were launched from the United States and the export of the spacecraft is otherwise eligible for export via STA. Additionally it would seem to impose an unnecessary and overly burdensome requirement for additional licensing for typical situations in which US persons were to take control of a satellite overseas for the purpose of initial operational testing and/or in-orbit testing. Such situations should not require a license if the title and ownership of the satellite does not change.

Recommendation: Revise §734.13(a)(3) to read as follows:

§ 734.13 Export.

(a) Except as set forth in § 734.17, “export” means:

(3) Transferring by a person in the United States of registration or ownership of a spacecraft subject to the EAR to a person in or a national of any other country; or. . .

IV. ITAR §120.46 / EAR §772.1: Required

The newly proposed definition for “Required” as it relates to Technical Data aligns to the existing EAR and Wassenaar Arrangement definitions, which is a positive development. In particular, the addition of Note 2 to §120.46 & §772.1 to align the Technical Data category with the commodity that it represents will increase consistency and aid in making the regulation more intuitive.

Peculiarly Responsible: However, the addition of Note 3 to § 120.46(a) that defines the term “peculiarly responsible” is unnecessary and overbroad. Under the proposed rule, all technical data peculiar to, “the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article” would be controlled unless it satisfies relatively narrow exceptions.

Recommendation: A more effective mechanism for defining “peculiarly responsible” would be to provide an example or language that indicates that not all “technical data” which is required to produce a controlled item is “peculiarly responsible.” Rather, only those technologies that are added or combined in such a way to enable achieving or exceeding controlled performance levels, characteristics, or functions should be considered “peculiarly responsible.”

V. ITAR §120.52 Activities that are not exports, reexports, or retransfers

The proposed treatment for storage of encrypted data as a non-export activity is a positive regulatory construction. There are, however, several issues that warrant further review:

Transmission through a §126.1 Country: A potential barrier to implementation is the risk that data may be transmitted through, and thereby stored, in a ITAR §126.1/EAR D:5 country or Russia. The challenge is securing the “knowledge” that information entered in a virtual environment (i.e., cloud) is not transiting prohibited terrestrial boundaries. This requires verification of the location of operations and all employees with all potential service providers that support virtual environments, which may not be possible.

“End-to-End” encryption: Information technology security is often a layered approach, and it is possible that multiple levels of encryption, both system or user base, exist requiring decryption keys, network access codes, or passwords for access.

Introduction of Multiple Standards: Multiple standards for encryption introduces complexity (i.e., §120.52 of the ITAR; §734.18 of the EAR, and potentially in the DFAR). Without agreement on a single standard, companies must evaluate the highest standard or attempt to manage information by multiple standards, which diminishes the overall intent to harmonize regulation – increasing both risk and cost.

Jurisdiction: Changing jurisdiction and classification of decryption keys, network access codes, or passwords based on the contents of the encrypted repository is problematic. The current definition of Technical Data continues to provide the consistent standard for what is controlled and for what is a violation under §127.1/§ 764.2, which include the unauthorized visual, oral, written or other inspection of technical data. If the concern is that the four terms used in release do not adequately define the risk for data exfiltration, then the USG should consider broadening the definition of release to capture those actions which identify the transfer without inspection.

Non-Exports: Additionally, providing decryption keys, network access codes, or passwords that would allow access does not constitute a transfer or export since these items are not identified on the USML. If a company is able to forensically prove that these items/data were not transferred or inspected by a foreign party, then it should not constitute an export. The result of investigation and a robust compliance program should be sufficient to review the situation for corrective action and prevent violations.

Double Jeopardy: The broadening of the Technical Data definition to include “decryption keys, network access codes, or passwords” has the potential to characterize a single violation as both the unauthorized release of the technical data and a secondary violation for the release of decryption keys, network access codes, or passwords when an unauthorized foreign party accessed that technical data. The unintended consequence is that the USG enforcement elements now have to account for duplicate violations for a single infringement.

Without addressing these concerns, the proposed regulation will not achieve the goal of defining an acceptable standard for release. To the contrary, the risk and uncertainty may force companies to restrict or eliminate virtual environment (i.e., cloud) as an option for storing data.

Recommendations:

- Reconsider the standard for the release of the decryption keys, network access codes, or passwords as an export in and of itself in sections 120.52 and violation in § 127.1(b)(4).

- Provide further clarification of End-to-End Encryption in light of the fact that it is not uncommon for system or service/third party providers to store decryption keys, network access codes, or passwords for user's accounts in virtual environments.
- Provide a single encryption standard that is identified within the ITAR, EAR, and DFAR.
- Revise or delete §120.10(a)(5)/§ 772.1(a)(5) and §127.1(b)(4)/ § 764.2(l) to revert the definition of Technical Data to the current standard.
- Lastly, include the names of inhabited territories, dependencies, or possessions (American Samoa, Guam, U.S. Virgin Islands, Wake Island) for easy reference in § 120.52(a)(3).

VI. ITAR §120.47: Development

Design Concepts: Design concepts are representative approaches that may or may not meet necessary performance thresholds subject to control under the USML. Concepts have not yet been confirmed through analyses to meet USML control thresholds and are therefore more indicative of general system descriptions than controlled articles.

Recommendation: Delete “design concepts” from the definition of Development.

VII. ITAR §120.48: Production

Production vs. Manufacturing: The addition of the Production definition may expose some of the existing confusion with the term as it is used elsewhere within the ITAR. The new definition of Production is broader than manufacturing and includes manufacturing as only one part of the production process. The §120.21 definition of Manufacturing License Agreement is limited to granting “a foreign person an authorization to manufacture” defense articles. §120.21 does not stipulate that a Manufacturing License Agreement is required if production rights are granted. Likewise, the definition of Technical Assistance Agreement adds more confusion to the situation. In addition, the definition of Production includes assembly, provided that production rights are not transferred. This creates an inconsistency between the definition of Technical Assistance Agreement and the new definition for Production.

The provisions of §124.4(b)(1)-(4) currently apply to Manufacturing License Agreements. The current inclusion of production within the reporting requirement and the broader association to activities beyond manufacturing may cause confusion, potentially increasing the burden by requiring agreement holders to unnecessarily file §124.4(b)(1)-(4) reports for a subset of Technical Assistance Agreements.

Recommendation: Modify §124.4(b) as follows:

§124.4 Deposit of Signed Agreements with the Directorate of Defense Trade Controls
(b) In the case of concluded agreements involving licensed manufacturing of United States origin defense articles outside of the United States, a written statement must accompany filing of the concluded agreement with the Directorate of Defense Trade Controls, which shall include:

- (1) The identity of the foreign countries, international organization, or foreign firms involved;
- (2) A description and the estimated value of the articles authorized to be manufactured, and an estimate of the quantity of the articles authorized to be produced;
- (3) A description of any restrictions on third-party transfers of the foreign manufactured articles; and
- (4) If any such agreement does not provide for United States access to and verification of quantities of articles manufactured overseas and their disposition in the foreign country, a description of alternative measures and controls to ensure compliance with restrictions in the agreement on manufactured quantities and third-party transfers.

CONCLUSION

Thank you for the opportunity to provide comments in response to the proposed rules. Lockheed Martin remains committed to supporting the ongoing effort to reform and improve the U.S. export control system. We are confident that the changes recommended above will have a positive impact on our ability to support U.S. national security and foreign policy priorities by harmonizing definitions and aligning compliance standards for U.S. export controls.

If you have any questions related to these comments or would like additional information related to the issues discussed above, please contact Mark Webber, Director, International Trade Policy, Government & Regulatory Affairs at 703-413-5951 or Mark.J.Webber@lmco.com.

For Lockheed Martin,



Mark J. Webber
Director, Government & Regulatory Affairs



PATRICK SCHLESINGER
ASSISTANT VICE CHANCELLOR
RESEARCH ADMINISTRATION AND COMPLIANCE

2150 SHATTUCK AVENUE, SUITE 300
BERKELEY, CA 94704-5940
TEL: (510) 642-2866/FAX: (510) 642-8236
EMAIL: PSCHLESINGER@BERKELEY.EDU

August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
PM/DDTC, SA-1, 12th Floor
Washington, DC 20522

Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW
Washington, DC 20230

Re: (RIN 1400-AD70 and RIN 0694-AG32)
Comments on Proposed Revisions to ITAR and EAR Definitions

Dear Mr. Peartree and Ms. Hess:

The University of California, Berkeley (“Berkeley”) appreciates the opportunity to comment on the proposed amendments to the International Traffic in Arms Regulation (ITAR) and to the Export Administration Regulations (EAR), which are designed to harmonize the two sets of definitions, and which are published at 80 Fed. Reg. 31525 and 80 Fed. Reg. 31505 (June 3, 2015).

Berkeley supports and incorporates by reference comments submitted by the University of California’s Office of the President, the Association of University Export Control Officers (AUECO), the Association of American Universities, the Council on Government Relations, and the American Bar Association’s Section of International Law. As with the other commenters, Berkeley appreciates the efforts that State and Commerce have made to remove substantive differences between the two regulatory schemes. However, we agree with the other commenters that additional work is required.

Definition of Fundamental Research

Berkeley supports State’s decision to separate “fundamental research” from the definition of “public domain” and the recognition in both the EAR and ITAR that fundamental research should include information that “arises during, or results from, fundamental research.” However, Berkeley agrees with other commenters that the description of fundamental research that appears in the jurisdictional language of §120.6 should carry through to §120.49.

Berkeley also agrees that a serious problem exists is the current form of §120.49(b). As drafted, the technical data that arises during, or results from, fundamental research and that is intended to be published only qualifies to the extent that the researchers are free to publish the “technical data” contained in the research “without any restriction or delay”, including “U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.” (Emphasis added.) This approach is not harmonized with the EAR and is completely at odds with the way

DDTC, the Department of Commerce, and the Department of Defense have interpreted the concept of fundamental research since it was first adopted in the EAR and ITAR.

NSDD-189 distinguishes fundamental research, the results of which are published and shared broadly within the scientific community, from proprietary and restricted research, the results of which are restricted for proprietary or national security reasons. The key point is the restriction. As described in the EAR §734.8(b)(2), “[p]ublication review by a sponsor of university research solely to insure that the publication would not inadvertently divulge proprietary information that the sponsor has furnished to the researchers does not change the status of the research as fundamental research.” Similarly, the EAR provides that “[p]ublication review by a sponsor of university research solely to ensure that the publication would not compromise patent rights does not change the status of fundamental research, so long as the review causes no more than a temporary delay in publication of the research results.” (15 CFR §734.8(b)(3)) As with the other commenters, Berkeley acknowledges that when proprietary technical information is furnished by outside sources, the furnished data and any derivative data do not fall under the same protected status as the data resulting from fundamental research.

Berkeley agrees with the other commenters that the proposed rule confuses two very different concepts. In the case of governmental access and dissemination controls, the government does not simply review a research publication but makes a decision to approve the publication for public release or to restrict the release based on national security considerations. Industry sponsors of university fundamental research insist on reviews simply to ensure that none of the company’s proprietary material has made its way in to the research report before it is published and to give it a brief opportunity to decide whether the research has resulted in any patentable inventions. Once any proprietary material is removed and it has made its patenting decision, the company has no further interest in controlling or restricting the publication. If, by contrast, the research sponsor has reserved for itself the ability to restrict the research for proprietary reasons and will use the research results for proprietary purposes, then it no longer qualifies as fundamental research under NSDD-189, the EAR (present or revised), or the present version of the ITAR.

If the §120.49(b) language were to be adopted in its present form, this would prevent Berkeley from performing fundamental research of interest to industry in areas in which it might use such fundamental research results in its own industrial development activities under ITAR. This is because industry always insists on a prepublication review to ensure that no proprietary information has been included in the final publication. Today, such prepublication review does not destroy the fundamental research character of the activity. Under §120.49(b) as proposed, it would.

At the beginning of the proposed rule, the Department notes that it will harmonize certain terms under the ITAR with terms under the EAR to the extent appropriate. Berkeley acknowledges that it may not be possible to make all of the definitions identical under the two sets of regulations due to differences in the underlying reasons for control of items on the U.S. Munitions List or Commerce Control List. However, because information arising during, or resulting from, fundamental research is publicly available and shared broadly in the scientific community, and therefore should not be subject to control under either set of regulations, there is no reason not to harmonize the definition of “fundamental research” across both regulatory regimes.

Definition of Educational Information

In the EAR §734.9 and various parts of the ITAR, including §120.6(b)(3)(iii) and the note to paragraph (a) in §120.9(a), the agencies have exempted application of the restriction EAR and ITAR restrictions to educational information when it concerns “general” scientific, mathematical, and engineering principles that are “commonly” taught in schools. Berkeley believes that this unduly limited in several respects. As other commenters have noted, the definition raises the concern that the exemption does not apply to current and innovative courses. In addition, because the definition of “applied research” within the definition of fundamental research in §120.49(c)(2)(ii) covers processes and techniques, these activities should be carried over into the context of educational activities. Berkeley believes that educational information

C. Edward Peartree
Hillary Hess
August 3, 2015
Page 3 of 3

should include instruction in “scientific, mathematical, or engineering principles, processes, and techniques taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution.”

Definitions of basic research, applied research, and development

Berkeley appreciates the efforts of State and Commerce to clarify the distinctions between “basic research” and “applied research” within fundamental research in §120.49(c) and §734.8(c) and “development as defined in §120.47. However, Berkeley also supports AUECO’s recommendations for revisions to “applied research.”

Definition of public domain

Berkeley also agrees that the definition used for “public domain” in the proposed regulations should follow the statements contained in the regulatory preamble. The revised §120.11 definition for “public domain” includes information that is submitted to co-authors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings for review for publication. The preamble to the proposed change states that this includes information that is submitted for review prior to actual publication. However, the revised §120.11(a)(5) appears to require that information also be accepted for publication to qualify as “public domain”. Berkeley believes that the language should be changed to clarify that information submitted for review for publication qualifies as “public domain” under §120.11(a)(5) regardless of acceptance for publication or actual publication. This clarification would allow information that is not favorably received or actually published to still qualify as “public domain.”

Respectfully submitted,

Patrick Schlesinger
Assistant Vice Chancellor
Research Administration and Compliance

July 15, 2015

To: DDTCPublicComments@state.gov
publiccomments@bis.doc.gov

From: Bill Root, waroot23@gmail.com; tel. 517 333 8707

Subject: ITAR Amendment - Revisions to Definitions: Data Transmission and Storage
EAR Revisions to Definitions - RIN 0694-AG32

The June 3, 2015 proposed rules from the State and Commerce Departments are intended to harmonize and clarify ITAR and EAR definitions while improving national security. These comments describe many respects in which they go in the opposite direction. The six most important ones are those numbered 1 to 6 below. Those numbered 7 to 10, while less important, are still significant. At the end is an analysis of what could happen if no changes are made.

1. Prior Restraint of Public Domain Exclusion from Export Controls

The ITAR proposed requirement for USG authorization to put information into the “public domain” in 120.11(b) is a reversal of actions 30 years ago to comply with the free speech first amendment to the Constitution. EAR proposals would change “are already published or will be published” to “are published” in what is “not subject to the EAR” in 734.3(b)(3)(i) and delete “The EAR do not cover technology ... that is made public by the transaction in question” now in 734 Supplement 1. So, ITAR would explicitly challenge the Constitution and EAR would remove language which now complies with the Constitution. Remedies: Delete 120.11(b); do not revise 734.3(b)(3)(I); and do not delete 734 Supplement 1.

2. Deletion of Clarifications

The many clarifying questions and answers concerning publicly available information in EAR 734 Supplement 1 would be deleted. Remedies: Do not delete 734 Supplement 1 (a few revisions to update that Supplement are included in #10 below).

3. Over-riding “Required”

ITAR 120.46 would add the EAR and Wassenaar definition of “required” as

“only that portion of technical data that is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions.”

However, per proposed Note 3, those words would ambiguously be met if technical data are for development, production, or use of a defense article unless subject to three releases now in the definition of “specially designed.” EAR would add to 772.1 a definition of “peculiarly responsible” having the same effect as ITAR Note 3. “Peculiarly responsible” wording now appears not only in the definition of “required” but also in the definition of “specially designed.” So, the June 3 proposals largely over-ride the substance of the “required” definition in ITAR and in the hundreds of existing uses of “required” and “specially designed” in the EAR. Remedy: Limit 120.46 Note 3 and 772.1 definition of “peculiarly responsible” to License Exceptions (for details see #10 below).

4. Violations of NSDD 189

A 1985 National Security Decision Directive (NSDD) 189 specifies:

“where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. ... No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification ...”

The June 3 120.49, 734.8, and 734.11 proposals expand existing pre-publication review restrictions on federally-funded fundamental research other than classification. Remedy: Delete all restrictions on federally-funded fundamental research in 120.49, 734.8, and 734.11 (for details see #10 below).

5. Inadequate Control of Munitions Production

Instead of expanding unconstitutional and unenforceable controls on what is publicly available and increasing ambiguity on what technology is controlled, the United States should comply with the vastly more important multilateral controls on munitions production (WA ML 22.b.1) and missile production (MTCR 1.B.1). Several decades ago, a UK firm, Matrix Churchill, after consulting with the UK government, exported to Iraq, without a license, equipment not requiring a license but used to produce munitions. Parliamentarians severely criticized the UK government, which survived a motion of no confidence by just one vote. The UK had failed to include on its control list the following COCOM Munitions List item 22.b.1, which remains on the Wassenaar Munitions List to this day:

Design of, assembly of components into, and operation, maintenance, and repair of complete production installations for Munition List items even if the components of such production installations are not specified.

ITAR 120.9 defense services cover “furnishing assistance to foreign persons in the production of defense articles.” This is relevant. But, in 1980, DOD concluded that such general wording was insufficient. So, I led a negotiation which added ML 22.b.1. The Matrix Churchill case proved that DOD was right. Even so, in the intervening 35 years, neither State nor Commerce has seen fit to incorporate into a U.S. export control list WML 22.b.1, b.2, or b.5. WML 22.b.2 reads:

Technology required for development or production of small arms even if used to produce reproductions of antique small arms.

WML 22.b.5 reads:

Technology required exclusively for incorporation of biocatalysts specified in ML7.i.1 into military carrier substances or military materials.

In 1987, the Missile Technology Control Regime was established. Its main objective was to control production of missiles. Once again, ITAR defense services language was relevant. But U.S. negotiators wanted something more specific, called “production facilities,” defined as:

Production equipment and specially designed software therefor integrated into installations for development or for one or more phases of production.

Item 1.B.1, “production facilities” for missiles, has been on the MTCR list for almost three decades. But it still has not made it onto a U.S. export control list.

Remedies: add new ECCN 9B110 “Production facilities” for “development” or “production” of “missiles”; revise 9E018 heading to read “Technology” from Wassenaar Munitions List; and add 9E018 sub-items for WML 22.b.1, b.2, and b.5.

6. Discrepancies in prohibited countries between ITAR and EAR

The ITAR list of prohibited countries in 126.1 is supposed to be replicated in EAR Country Group D:5. A footnote to D:5 states that, if there are any discrepancies between the two lists, the State Department list shall be controlling. On January 29, 2015, BIS added an embargo of Crimea to EAR 746.6, except for food and medicine, but did not add Crimea to D:5. DDTC has not yet added Crimea to 126.1. It makes no sense to prohibit to Crimea toothpaste and paper clips, but not items on the USML. On May 29, 2015, the State Department removed Fiji from 126.1. D:5 still includes Fiji. Remedies: add Crimea to 126.1 and to 740 Supplement 1 Country Group D:5 and delete Fiji from D:5.

7. Establish new ITAR sections of part 120 to read:

Subject to ITAR

- (a) Except for items excluded in paragraph (b) of this section, the following items are subject to the ITAR:
 - (1) All USML-controlled “commodities,” software, and “technology” (*i.e.*, all “defense articles” and “defense services”) located in the United States, including in a U.S. Foreign Trade Zone or moving in-transit through the United States from one foreign country to another; and
 - (2) All U.S.-origin “defense articles” and “defense services” wherever located;
- (b) The following are not subject to the ITAR:
 - (1,2,3,4) (From proposed 120.6(b)(3)(i, ii, iii, iv), re public domain, fundamental research changing 120.46 to 120.49), scientific principles, and patents, and delete 120.6 Note to paragraph (b).
 - (a) and (b)(1-4) would harmonize with EAR 734.3(a)(1), (a)(2), and (b)(3).)
 - (5) Basic marketing information on function, purpose, or general system descriptions of defense articles;
 - (6) Telemetry data per XV Note 3.
 - ((b)(5) and (6) would harmonize with 120.10(b) exclusions from “technical data.”)

Commodity

Commodity means any item except software or technology.

(This would harmonize with the EAR definition of “commodity.”)

Technology

Technology means “technical data” or “defense services”

(This would harmonize with EAR and Wassenaar.)

8. Revise ITAR 120.6, 120.9, and 120.46 and EAR 772.1 definition of “peculiarly responsible,” as follows:

120.6 Defense article, revise to read:

Defense article means any commodity, software, or technical data controlled on the United States Munitions List.

120.9 Defense services:

In (a)(1) change “directly related to” to “required for”;

In Note 1 to paragraph (a)(1) change “directly related to” to “required for” (twice).

(This would harmonize with EAR and Wassenaar.)

120.46 Required:

In (a), change “technical data” to “technology” (three times);

In Note 2 to paragraph (a):

change “technical data” to “technology” (twice);

change “enumerated” to “controlled”;

change “to which it is directly related” to “for which it is required”; and

change “directly related to” to “required for”;

Revise Note 3 to paragraph (a) to read:

“Technology” “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions” is, nevertheless, not controlled if:

(1, 2, 3, 4, 5 from proposed Note 3)

(Recommended changes in paragraph (a), in Note 2 to paragraph (a), and to remove from Note 3 that technical data for a defense article is controlled regardless of the performance level, characteristic, or function would harmonize with EAR and Wassenaar.

Changing “enumerated” to “controlled” in Note 2 would retain on the USML technical data specifically described there using catch-all language excluded from enumerated.

The recommended retention in Note 3 of decontrol parameters would harmonize with the recommended portion of the BIS proposed definition of “peculiarly responsible.”)

772.1 peculiarly responsible, revise to read:

“Technology” “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions” is, nevertheless, not controlled if:

(1, 2, 3, 4, 5, 6 from proposed definition)

9. In subcategories for technical data and defense services on the USML, change
 Technical data (see 120.10 of this subchapter) and defense services (see 120.9 of this subchapter) directly related to the defense articles described in ...
 to

Software “specially designed” for and “technology” “required” for “commodities” (and software) controlled by ...

10. Revise ITAR 120.11 and 120.49 and EAR 734.3, 734.7, 734.8, 734.11, Supplement 1 to part 734, and 740.9(c), as follows:

120.11 public domain:

In (a) insert following new (a)(1) and renumber (2) through (5) as (3) through (6):

(1) Sales at a price not exceeding the cost of reproduction and distribution;

Delete 120.11(b)

120.49 fundamental research

In (a)(1), delete “located”

Add the following new Note 3 to paragraph (a):

Pursuant to NSDD 189, where the national security requires control of information generated during federally-funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories, the mechanism for control is classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification.

Delete and Reserve 120.49(b) (on prepublication review) and delete the three Notes to paragraph (b)

(Proposed Note 2 to paragraph (a) provides adequate guidance for privately sponsored fundamental research. Recommended Note 3 to paragraph (a) provides adequate guidance for federally-funded fundamental research.)

734.3(b)(3)(i):

change “Are “published”,” to “Are already published, or will be published”; and

add: “(the EAR do not cover technology that is already publicly available, as well as technology that is made public by the transaction in question)”

734.7 Published

In (a) insert following new (a)(1) and renumber (2) through (5) as (3) through (6):

(1) Sales at a price not exceeding the cost of reproduction and distribution;

734.8 fundamental research

after the semi-colon at the end of (b)(1), add “or”

at the end of (b)(2), change “; or” to a period

delete (b)(3); delete Note 2 to paragraph (b); insert following new (c), reletter (c) to (d)

(c) Pursuant to NSDD 189, where the national security requires control of information generated during federally-funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories, the mechanism for control is classification. No restrictions may be placed upon the

conduct or reporting of federally-funded fundamental research that has not received national security classification.

734.11 Government-sponsored research covered by contract controls

Delete

734 Supplement 1 Questions and answers - technology and software subject to the EAR

Retain, rather than delete as proposed

Delete Question A(4) Research under DOE grant requiring prepublication DOE clearance

Delete Answer to A(6) and substitute:

No, provided that:

the government has not classified any of its content;
 you did not include, or otherwise use, any classified information in its preparation;
 your intent is to make it available generally to the public;
 during its preparation, you agreed to no private pre-publication review; and
 you have not sold it, or advertised it for sale, at a price exceeding the cost of reproduction and distribution.

Delete Answer to D(11) and substitute:

Yes, provided that:

the government has not classified any of its content;
 you did not include, or otherwise use, any classified information in its preparation;
 your intent is to make the research available generally to the public;
 during its preparation, you agreed to no private pre-publication review; and
 you have not sold it, or advertised it for sale, at a price exceeding the cost of reproduction and distribution.

Delete Answer to E(1) and substitute:

Pursuant to 120.49 Note 3 to paragraph (a) and 734.8(c) (as recommended above), the only permissible restriction on federally-funded fundamental research is classification. You should ask the DOD sponsor to withdraw the prepublication review requirement.

Delete 740.9(c) beta test software

(The expressions “intended for distribution to the general public” and “free-of-charge or at a price that does not exceed the cost of reproduction and distribution” make this “not subject to the EAR,” so that no license exception is needed.)

Analysis

Imagine you are a journalist writing a story on the impact of U.S. bombers in Iraq and Syria. You read in Note 1 to paragraph (a) of 120.46, on “required,” that “any technical data, regardless of significance, peculiar to making an aircraft a bomber” is controlled. Almost anything you write about a bomber could be construed as somehow related to making it. You clearly intend to put

your story in the public domain. But you note removal of sales at newsstands from the definition of public domain. Moreover, you read in 120.11(b): “Technical data or software, whether or not developed with government funding, is not in the public domain if it has been made available to the public without authorization from (a U.S. government official).” So you seek such authorization. You then discover that, for similar reasons, not only newspapers in general but also other media, advertising agencies, and academic researchers are also seeking such authorizations, often for their entire content, out of an abundance of caution. The government is overwhelmed and cannot respond within the deadlines demanded by the applicants. Moreover, the courts cannot cope with the deluge of lawsuits alleging unconstitutional prior restraint of free speech. So, reporters, advertisers, and researchers, not wishing to stop their vocations nor to significantly delay publishing, advertising, or sharing research results with the public, feel obliged to make their information publicly available without government authorization. They would thereby incur the risk of “administrative, civil, and possible criminal penalties under other law,” per 734 Supplement 1 E(2). This quotation would be deleted but would probably still be applicable.

The proposed 772.1 definition of “peculiarly responsible” would ambiguously over=ride the substance of the existing Wassenaar and EAR definition of “required” and a key part of the EAR definition of “specially designed.” Those terms are used in hundreds of places in the CCL. The ambiguities would cause incredible confusion in industry. Exporters would inevitably make varying interpretations. These are national security rules. Such confusion would be a significant threat to national security. That threat can easily be avoided by simply retaining the existing definitions of “required” and “specially designed” unchanged.

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC 20230

Sent via email to publiccomments@bis.doc.gov, subject "RIN 0694-AG32"

MIT appreciates the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*.

We support the efforts of the Departments of Commerce, Defense, and State to rationalize, clarify, and focus U.S. export controls. RIN 0694-AG32 and the accompanying RIN 1400-AD70 regarding revisions to ITAR definitions, include elements of progress toward harmonized and constructive definitions of terms. The exclusions to end-to-end encryption are a welcome change and will reduce administrative burden to the academic community, and BIS's confirmation of our understanding of the definition of fundamental research is very helpful. However, the proposed rule contains several other changes that would significantly hamper MIT's ability to achieve its missions of delivering high quality cutting edge education to its students, and maintain its leadership position as a world-class research and educational institution.

- Design laboratories are an integral part of technical education, particularly in capstone classes that help students integrate learning from separate subject areas. Under the proposed rule, these courses could be seen as going beyond "general principles" and be subject to the EAR, thereby restricting course participation based on nationality. This would violate MIT's "open university" policy without any evidence that these classes present risks to nationalist security.
- MIT researchers typically publish both the research results ("technology") and software resulting from fundamental research. The proposed rule would limit researcher's ability to publish the software. Both the results and any software resulting from fundamental research should be publishable under the EAR.

The above issues and responses to the questions asked in the proposed rule are discussed in detail below. Revisions are provided where appropriate.

Responses to issues for which BIS solicited comments:

1. Whether the proposed revisions create gaps, overlaps, or contradictions between the ITAR and EAR, or among various provisions within the EAR

Prepublication review of fundamental research: The changes to the ITAR proposed in RIN 1400-AD70 §120.49(b) Prepublication Review are significantly different from the EAR proposed rules, and discussed further in “Effective date” below.

2. Whether the proposed alternative definition of fundamental research should be adopted

MIT welcomes BIS’ proposed alternate definition of “fundamental research”, which increases clarity while remaining consistent with NSDD-189: “Fundamental research’ means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.”

To address the undefined term “non-proprietary”, MIT proposes a minor revision:

Proposed alternate definition of fundamental research

“Fundamental research’ means research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.”

This definition is objective, consistent with NSDD-189 (and with the intent of BIS’ proposed alternative), and does not rely on the additional defined terms “basic research” and “applied research”, which have multiple definitions in different areas of Federal regulations and are open to varying interpretations.

3. Whether the proposed alternative definition of applied research should be adopted

The proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18). This would be further clarified by including the entire definition, which adds “for sale” as a criterion. The additional text is bolded below.

Proposed complete DFARS definition of applied research

“Applied research,” means the effort that:

- (i) Normally follows basic research, but may not be severable from the related basic research;
- (ii) Attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or technique; and
- (iii) Attempts to advance the state of the art.

Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development [defined in 48 CFR part 31.205-18]

4. Whether questions and answers in Supplement No. 1 to Part 734 include criteria that should be retained

MIT urges BIS to retain the questions and answers found in Supplement No. 1 to part 734 in the regulations. While we agree that the questions and answers are illustrative, including them in the EAR has provided stability, minimizing differences in interpretation that occur outside the rulemaking process. We are concerned that removing the questions and answers would create increased uncertainty in our application of key concepts including fundamental research, publication, and educational instruction.

5. For End-to-end encryption, what standards should be adopted and should EAR and ITAR have the same standards

Excluding the sending, taking or storing of technology or software that is secured using end-to-end encryption from control as exports is welcome to the academic research community. It will reduce faculty burden associated with international travel and the use of main campus resources while abroad.

8. What should the Effective date for any changes to the regulation

We assume RIN 0694-AG32 and the accompanying RIN 1400-AD70 would take effect concurrently.

It would not be possible for universities to meet the compliance obligations imposed by the addition of the republication review language of ITAR §120.49(b) within 30 days of the publication date.

An extension would not relieve the basic problem: the effect of this change would be crippling to research sponsored by industry and foundations. As described above, this would force universities to choose among bad alternatives, all of which are inconsistent with the role university research has had in advancing U.S. innovation and competitiveness.

Fundamental Research

§734.3(b)(ii) and §734.8

The proposed §734.3(b)(ii) states that “information and ‘software’ that arise during, or result from, fundamental research, as described in §734.8 ... are not subject to the EAR”.

However, the referenced §734.8 is titled “‘Technology’ that arises during, or results from, fundamental research”. This change from “information and software” in §734.3(b)(ii) to “technology” in §734.8 creates several problems:

- §734.8 doesn’t cover the “information and software” referred to in §734.3(b)(ii). “Technology” is only a subset of information (§772.1), and “technology” doesn’t include “software” (§734.3(b)(ii)).
- Fundamental research doesn’t create “technology”. “Technology” is a defined subset of information subject to the EAR (§772.1). The results of fundamental research — information and software — are not subject to the EAR §734.3(b)(ii).

- University research would be complicated and restricted if “fundamental research” doesn’t include software. That would mean that natural-language documents written by a researcher would be “technology” that could be freely shared, but computer-language documents (software) written by the same researcher, would be subject to deemed export restrictions.
- “Published” treats “software” like “technology” (§734.7(a)), and “deemed export” treats software “source code” the same as “technology” (§734.13(b)) —recognizing that software is a publishable, communicable creation of human thought like other information.
- NSDD-189 speaks of fundamental research “results ... which ordinarily are published and shared broadly within the scientific community”. The language in §734.3(b)(ii) is consistent with this; the language in §734.8 is not.

MIT strongly recommends that the language of §734.3(b)(ii) be reflected in §734.8.

Proposed change to §734.3(8):

§734.8 Information and software that arise during, or results from, fundamental research.

(a) Information or software that arise during, or results from, fundamental research and is ‘intended to be published’ is thus not ‘subject to the EAR.’

(b) Prepublication review. Information or software that arise during, or result from, fundamental research is “intended to be published” to the extent that the researchers are free to publish the information or software contained in the research without restriction or delay. Information that arises during or results from fundamental research subject to prepublication review is still “intended to be published” when: ...

Note: information that arises during, or results from fundamental research includes software

Removal of specific criteria (current §734.8(b)):

MIT appreciates that the proposed definition of “fundamental research” clarifies its broad applicability regardless of organization type or location. However, U.S. universities have found the specific criteria for university based research (current §734.8(b)) helpful in evaluating proposed research activities and using paragraphs 2 – 6 to help reach reliable determinations of whether the research qualifies as “fundamental research” under the EAR.

We recommend that the specific language of §734.8(b) be retained in the EAR. If this is not possible, we suggest that BIS develop a decision tree tool for universities that incorporates the current criteria for university based fundamental research.

Education

§734.3(b)(iii)

Some university catalog courses would become subject to the EAR under the proposed rule, although the preamble states that “this proposed rule is not intended to change the scope of the current §734.9.”

Under the current EAR, technology and software that are released by instruction in a catalog course or associated teaching laboratory of academic institutions are not subject to the EAR (§734.3(b)(3)(iii) and §734.9).

The proposed §734.3(b)(iii) adds two constraints, by stating that “information and ‘software’ that ... concern general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities, and released by instruction in a catalog course or associated teaching laboratory of an academic institution” are not subject to the EAR.

Design laboratories are an integral part of technical education, particularly in capstone classes that help students integrate learning from separate subject areas — these could be seen as going beyond “general principles” and subject to the EAR. Leading universities provide curriculum innovation by introducing new courses — these could be seen as not “commonly taught” because they’re innovative, and subject to the EAR.

Education at universities is by nature open, limited only by prerequisite knowledge, not by citizenship or national origin. A narrow interpretation of the proposed §734.3(b)(iii) would inhibit U.S. universities’ ability to develop new courses, and to continue to offer knowledge-integrating educational experiences areas of science and engineering that are critical to the future competitiveness of the industrial sector.

MIT believes that the national interest would be best served by deleting “concern general scientific, mathematical, or engineering principles commonly taught in schools” from the proposed §734.3(b)(3)(iii), which would harmonize with the current EAR definition.

MIT recommends deleting “concern general scientific, mathematical, or engineering principles commonly taught in schools” from the proposed §734.3(b)(3)(iii), which would retain the current EAR definition.

Proposed change to §734.3(b)(3)(iii):

“(iii) Released by instruction in a catalog course or associated teaching laboratory of an academic institution.”

MIT appreciates the opportunity to provide BIS with the above comments on RIN 0694-AG32.

Sincerely,

Maria T. Zuber

Linda Dempsey

Vice President

International Economic Affairs

August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C.

Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C.

Re: Revisions to Definitions in the Export Administration Regulations (RIN 0694-AG32)
Via e-mail: PublicComments@bis.doc.gov

Re: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage (RIN 1400-AD70)
Via e-mail: DDTCPublicComments@state.gov

Dear Mr. Peartree and Ms. Hess:

The National Association of Manufacturers (NAM) welcomes the opportunity to comment on the proposed rules to revise definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). The NAM continues to support the President's Export Control Reform Initiative, and we view the harmonization of definitions across the ITAR and EAR as a critical step in the initiative that will encourage consistency of classification and application.

The NAM is the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states. Our members play a critical role in protecting the security of the United States. Some are directly engaged in providing the technology and equipment that keep the U.S. military the best in the world. Others play a key support role, developing the advanced industrial technology, machinery and information systems necessary for our manufacturing, high-tech and services industries.

The proposed rules would amend the ITAR and EAR to update key definitions – including “defense article,” “defense services,” “technical data,” “public domain,” “export,” and “reexport or retransfer,” “peculiarly responsible,” “proscribed person,” “published,” results of “fundamental research” and more – in order to clarify the scope of activities and information that are covered within these definitions, as well as to harmonize the definitions. Additionally, the State Department proposes to create several definitions – including “required,” “technical data that arises during, or results from, fundamental research,” “release,” “retransfer,” and “activities that are not exports, reexports, or retransfers” – in order to clarify and support the interpretation of the revised definitions that are proposed in this rulemaking. The State Department also proposes to address the electronic transmission and storage of unclassified “technical data” via foreign communications infrastructure, proposing that the electronic transmission of unclassified “technical data” abroad is not an “export,” provided that the data is sufficiently secured to prevent access by foreign persons.

Leading Innovation. Creating Opportunity. Pursuing Progress.

Definition of “Export”

EAR §734.2(b) currently has definitions for export, export of technology or software, and export of encryption source code and object code software. Section 772.1 also defines “export” as follows: “Export means an actual shipment or transmission of items out of the United States.” The Commerce Department rulemaking proposes to consolidate the definitions of “export” and “export of technology and software,” while moving “export of encryption source code and object code software” to a new §734.13. The State Department proposes to revise the definition of “export” in ITAR § 120.17 to better align with the EAR's revised definition of the term and to remove activities associated with a defense article's further movement or release outside the United States, which will now fall within the definition of “reexport” in §120.19. The proposed rule also explicitly references the new §120.49, “Activities that are Not Exports, Reexports, or Retransfers,” which excludes from ITAR control certain transactions identified therein.

Manufacturers are concerned with the proposed wording of the proposed §734.13(a)(6), which is written to include knowledge that “will cause or permit” the transfer of other “technology” in clear text or “software” to a foreign national. The implication of this revision is that management of computer systems by non-U.S. persons would be prohibited if the data is stored in readable form, or “clear text.” We encourage the Commerce Department to avoid this result by adopting similar definitions to those found in §734.18(a), §734.18(b) and §734.18(c), as “Activities that are not exports, reexports or transfers.” Otherwise, the only efficient way to utilize non-U.S. persons to manage computer systems that contain export controlled data would be to encrypt data files that go into the system and keep them encrypted while in the system. Currently, the Commerce Department allows for a management system where computer administrators don't access/read the data. The implementation of this rule as currently proposed would raise the compliance burden significantly.

In the ITAR definition of “export” in §120.17, we recommend revising §120.17(a)(6) to align the ITAR definition with the EAR definition by incorporating concepts of “knowledge” and “actual transfer” into the definition. Additionally, the proposed definition of “export” adds paragraph (b)(1) to state explicitly that the release of “technical data” to a foreign person is deemed to be an “export” to all countries in which the foreign person has held citizenship or holds permanent residency. This creates a divergence between the ITAR and the EAR, where §734.13(b) codifies a long-standing Commerce Department policy that when technology or source code is released to a foreign national, the export is “deemed” to occur to that person's most recent country of citizenship or permanent residency. Maintaining two different standards increases the regulatory burden on U.S. exporters and is inconsistent with the goal of the Export Control Reform Initiative to harmonize the two sets of regulations. We recommend modifying the proposed revision §120.17 to better align it with the EAR.

Definition of “Required”

We believe the State Department has over-complicated the definition of “required” by adding Note 3 to subsection (a) of § 120.46, providing a proposed definition of “peculiarly responsible.” Under the proposal, all technical data peculiar to “the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article” is initially caught, even if they are not responsible for achieving the controlled performance levels, characteristics or functions. Using a catch-and-release approach is potentially confusing for U.S. companies. We suggest the State Department instead more clearly illustrate the definition by providing an example, like that which is provided in the EAR.

The NAM appreciates the opportunity to provide comments on these complex issues. Manufacturers remain committed to working with the Department of Commerce and other U.S. agencies to improve and streamline U.S. export control requirements that will promote U.S. economic, national security and foreign policy interests.

Thank you,

A handwritten signature in black ink, appearing to read "Linda M. Dempsey". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Linda Dempsey

LMD/la

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

The University of Colorado Boulder ("CU-Boulder") welcomes the opportunity to provide comments regarding the proposed changes to the Export Administration Regulations (EAR). CU-Boulder has an extensive research portfolio, receiving \$425M in sponsored research funding in 2014-15, including \$52M from the Department of Commerce. We are also firmly committed to the role of public universities in collaborating in and sharing the results of fundamental research. Therefore, we have a significant interest in export control reform, and appreciate the efforts of the Departments of Commerce and State to harmonize definitions and procedures between the EAR and the ITAR. While much progress has been made, we also believe that there are further opportunities to hone these definitions in ways that both protect national security considerations and facilitate the research engine that significantly drives the national economy.

Below are our comments on the eight issues on which BIS has requested specific comments:

1. Whether the proposed revisions create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR.

Response: While we greatly appreciate the improved harmonization between the two sets of regulations, we do have a very strong concern about the difference in how the EAR and ITAR deal with prepublication review by sponsors. We are encouraged that the proposed ITAR rule recognizes that information arising during, or resulting from fundamental research that is "intended to be published" is not technical data subject to the ITAR, making the ITAR consistent with the EAR in this regard. However, it is deeply concerning that the proposed ITAR rule then differs from the EAR in providing that "intended to be published" does not apply to a research sponsor's review of proprietary information.

This provision, the basis of which is not explained, will have a major impact on university-industry collaboration precisely at a time when such collaboration is a priority for industry, academia, and the Administration. Agreements with industry sponsors

routine include provisions for proprietary information review. Industry reasonably wants to guard against inadvertent disclosure of proprietary information or trade secrets when research is published. This kind of information is immaterial to the fundamental nature of the research being conducted, so CU-Boulder willingly accepts this requirement, as long as the time period for review is limited (typically to 60 days) and the scope is limited so that our researchers are free to publish their findings. These agreements make it clear that the research results are fundamental research, and not proprietary to the company. This situation differs significantly from those rare situations in which the sponsor demands the right to approve publication of the research results. CU-Boulder policy prohibits such agreements without prior review and approval by both a faculty committee and the Chancellor; if a policy waiver is provided, we ensure that all university participants are aware that such research is not considered fundamental research.

The proposed changes to the ITAR are inconsistent with not only the EAR but also with NSDD 189, impose a very significant regulatory burden, impede integrative research with industry, and raise Constitutional questions about prior restraint on publication and academic freedom. We strongly urge that the ITAR be aligned with the EAR interpretation and definition of fundamental research.

We also have significant concerns about the proposed restatement of the "education information exemption." The restatement appears to merge current ITAR and EAR text to state that "information and software that ...concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." We recommend that the "and" be changed to "or" in this statement. Increasingly, and appropriately, university education addresses not only "general principles" but also the experiential, "hands-on" application of specific principles, processes and techniques. This is particularly apparent in teaching laboratories and graduate education. Especially in the STEM fields, this ensures that U.S. students remain on the cutting edge of new developments. Limiting this exemption to "general principles" is unnecessary and counter-productive.

In addition, limiting the educational information exemption to what is "commonly taught" creates an impediment to academic innovation. Universities that are developing new curricular additions should not be penalized for thinking outside the box. Moreover, the "commonly taught" criterion is antithetical to the goal of incorporating the latest research findings into the courses taught by the same faculty who are conducting that research. If the information is provided in a catalog course that should be sufficient to treat such information similar to information that arises during, or results from, fundamental research. Thus we recommend deleting "commonly" from the revised definition.

Another difference between the EAR and ITAR are the provisions related to government-sponsored research covered by contract controls (EAR 734.11). The proposed EAR rule essentially restates the current 734.11(a), which universities have found confusing. CU-Boulder prefers the ITAR language at 120.49(b) Note 3, suitably modified to apply to technology arising during or resulting from fundamental research. We also find the examples in 734.11(b) to be helpful and recommend that they be retained.

2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted.

Response: While we generally support the proposed alternative definition of

fundamental research as “non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community,” the term “non-proprietary” may inject new ambiguity. CU-Boulder endorses the recommended definition provided by the Association of University Export Control Officers (AUECO) that defines fundamental research as “research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons”.

The proposed changes to §734.8(a) include a note that software and commodities are not “technology resulting from fundamental research.” This seems to contradict §734.3(b)(3) and 734.7(a) that treat technology and software similarly. If that is the intent, excluding software from fundamental research would have a substantial impact on university research, and does not appear to be supported by any logical distinction between, for example, natural language and computer language documents authored on the same topic by the same researcher. We strongly recommend that software arising during, or resulting from, fundamental research should not be subject to the EAR.

We also perplexed that the current presumption in EAR 734.8(b) that university based research will be considered fundamental research appears to have been eliminated. There is no clear policy reason stated for this change. We urge BIS to restate the presumption in the final rule.

Finally, we have concerns about the proposed EAR 734.8 Note 1 to paragraph (a), which states: “The inputs used to conduct fundamental research, such as information, equipment, or software, are not “technology that arises during or results from fundamental research” except to the extent that such inputs are technology that arose during or resulted from earlier fundamental research.” This statement seems to attempt to draw a delineation between the conduct of research and the results of that research that is neither practical nor consistent with NSDD 189. We urge that this note be deleted.

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

Response: We are ambivalent about the proposed definitions of applied research. Universities routinely use, and are very familiar with, the OMB Circular A-11 definition, and suggest it be adopted. Alternatively, if the DFARS definition of applied research is adopted we agree with the recommendation of the Association of University Export Control Officers that it should also include the 48 CFR 31.205-18 description of what applied research is NOT. This would provide added clarification, including a more clear delineation between “applied research” and “development” activities.

4. Whether the questions and answers in existing Supplement no. 1 to part 734 proposed to be removed (to the BIS website) have criteria that should be retained in part 734.

Response: We have found these Q&A's to be extremely helpful, and in fact have incorporated them into our internal guidance documents. While we recognize that they would still exist under the proposed changes, we fear that they would not have the same

gravitas if removed from the EAR and placed on the website. Researchers greatly appreciate specific guidance, so this proposed change is a significant step backwards.

5. With respect to end-to-end encryption as described in the proposed rule (sec. 734.18), whether the illustrative standard in the proposed EAR rule also should be adopted in the ITAR; whether the safe harbor standard in the proposed ITAR rule also should be adopted in the EAR, or whether the two bodies of regulations should have different standards.

We greatly appreciate that the proposed changes to both the EAR and ITAR provide clarification regarding cloud computing. CU-Boulder prefers the proposed EAR definition in 734.13(a)(6), which requires actual knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. We also prefer the EAR provision in 734.18(4)(iii) providing for “other similarly effective cryptographic means” for securing technology or software. This provides useful flexibility now and, even more importantly, as technology advances.

We suggest that BIS consider adding a note that a contract that includes vendor restrictions on countries not proscribed in 126.1 is sufficient for compliance purposes. As a practical matter, ensuring actual compliance is beyond our effective control.

6. Whether encryption standards adequately address data storage and transmission issues.

Response: Our IT Security professionals need more time to explore this very complex issue.

7. Whether the proposed definition of "peculiarly responsible" effectively explains how items may be "required" or "specially designed" for particular functions.

Response: We have no comment on this proposed change.

8. The effective date of the final rule.

Depending on the extent of the final changes, the proposed 30-day delayed effective date creates a significant burden on CU-Boulder to ensure that all changes are implemented and promulgated to researchers. This short deadline creates particular challenges for researchers who are in the process of submitting proposals to funding sources. If the proposed changes regarding Prepublication Review go into effect without modification, substantial changes will be necessary to our business practices associated with review, negotiation, and management of sponsored research agreements. These changes will require implementation of new review procedures, including determination of whether the EAR or ITAR definition of “fundamental research” applies for research awards with sponsor review, development and monitoring of technology control plans, applications for export licenses, as well as revised export compliance training for researchers. To accomplish all of this will likely require hiring additional resources, which further adds to the timeline. To accommodate this panoply of changes will require at least a six-month delayed effective date.

CU-Boulder appreciates the work of the DDTC and BIS to harmonize their procedures, as well as the opportunity to provide comments on these proposed changes. We believe the proposed changes to the EAR are for the most part positive and worthy of support and hope that BIS will consider our comments when finalizing the definitions.

Sincerely,

A handwritten signature in black ink, appearing to read "Joseph G. Rosse". The signature is fluid and cursive, with the first name "Joseph" being the most prominent part.

Joseph G. Rosse, Ph.D.
Export Control Officer and Empowered Official



Sent electronically to publiccomments@bis.doc.gov

3 August 2015

Hillary Hess
Director, Regulatory Policy Division
Bureau of Industry and Security, Room 2099B
U.S. Department of Commerce
Washington, DC 20230

RE: Revisions to Definitions in the EAR (RIN 0694-AG32)

Dear Madam:

We applaud the U.S. Department of Commerce (DOC) for its efforts through the Export Control Reform Initiative to enhance clarity of Export Administration Regulations (EAR) definitions and establish consistency between EAR and terms found in the International Traffic in Arms Regulations (ITAR). We appreciate the opportunity to provide a formal response to the proposed revisions to the definitions of “fundamental research,” “technical data,” “technology,” and “public domain.”

With approximately 195,000 members residing in the United States, The Institute of Electronics and Electrical Engineers – USA (IEEE-USA) is an organizational unit of the Institute of Electrical and Electronics Engineers, Inc. (IEEE), the world’s largest organization for technical professionals, and a leading educational and scientific association for the advancement of technology. A large contingent of our membership in academe, industry, and commercial services conduct fundamental research and export technologies under the current EAR definitions.

In our analysis, the proposed definitions would unintentionally expand EAR’s authority to include research and technologies that are currently exempt. We strongly believe such an expansion in the increasingly competitive global technology market would unnecessarily impede progress in the research environment, restrict exports of technologies that do not possess dual-use characteristics, and ultimately jeopardize U.S. technological leadership.

With the understanding that this is not the intention of the DOC, IEEE-USA offers its analysis and provides several suggestions for improvement in the following pages. We would be happy to answer any questions you might have regarding our analysis or suggestions. We further offer to provide subject matter experts to assist in further development of these definitions, including leaders in fundamental research and technology development.

Fundamental Research

The BIS has requested comments on whether the alternative definition of fundamental research suggested in the preamble should be adopted.

Based on the analysis of IEEE-USA, presented below, the proposed language will impose new restrictions upon the conduct of fundamental research that is exempt under the current EAR definitions. DOC's proposed definition of "fundamental research" is:

"'Fundamental research' means nonproprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community."

IEEE-USA believes that the elimination of explicit reference to "basic" and "applied" research in the DOC's proposed definition would inadvertently subject certain fundamental research endeavors to the EAR. IEEE-USA believes that this conflicts with the spirit of the definition afforded in the National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical, and Engineering Information, which also does not reflect the character of modern fundamental research. The following are our principal concerns:

1. The "and" between "science" and "engineering" inherently implies that both terms need to be satisfied in order for the research to be deemed "fundamental." As DOC/BIS is aware, there exist fundamental research efforts that are purely scientific or purely engineering. To ensure sufficient clarity and coverage for all possibilities that encompass what is commonly accepted as fundamental research, the IEEE-USA recommends replacing the word "and" with "or" to read "science or engineering."
2. The proposed definition fails to acknowledge fundamental research of mathematical nature. While mathematics underpins science¹ and engineering², it also is embodied by and within mathematical algorithms, such as financial forecasting or cryptography. IEEE-USA recommends that the DOC either make clear that its use of the word "scientific" includes mathematics, or explicitly include the word "mathematics."
3. "Scientific community" excludes publishing or sharing broadly within the mathematical or engineering communities as well as the general public. The IEEE-USA suggests the DOC use the "research community or in the public domain" as alternate language to ensure the broadest acceptance of openly-available public information.

¹ Science is knowledge about the natural world that is based on facts learned through experiments and observation.

² Engineering is the application of scientific and mathematical principles to practical ends such as the design, manufacture, and operation of efficient and economical structures, machines, processes, and systems.

4. The IEEE-USA, therefore, suggests revised language, “Fundamental research’ means research in science, mathematics, or engineering, the results of which ordinarily are published or shared broadly within the research community or in the public domain.”

“Arises During or Results From”

The IEEE-USA is concerned over the proposed revision’s use of the description “arises during or results from fundamental research.” While the DOC intends to “make clear that technology that arises prior to a final result is subject to the EAR,” we believe that this has unintended consequences when combined with the proposed fundamental research definition, wherein the word “nonproprietary” is used.

Withholding the release of research results until the results are confirmed is general practices during the conduct of fundamental research. Without a specific definition for “nonproprietary,” IEEE-USA is unable to determine whether the proposed definition will constitute a problematic change to the EAR.

Applied Research

BIS has requested comments on whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

IEEE-USA supports the use of the National Science Foundation definition of applied research.

Applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.

IEEE-USA has significant concerns about the adoption of Defense Federal Acquisition Regulation (DFAR) Supplement (48 CFR part 31.205–18) for the definition of “applied research.” DFAR defines “applied research” to mean an:

“effort which (1) normally follows basic research, but may not be severable from the related basic research, (2) attempts to determine and exploit the potential of scientific discoveries or improvements in technology, materials, processes, methods, devices, or techniques, and (3) attempts to advance the state of the art.”

This proposed definition has many very significant failings that would negatively affect the conduct of fundamental research at large.

- First, the phrase “may not be severable from the related basic research” imposes a fundamental requirement to have a tie to basic research. While it is often the case that applied research follows from basic research, it is not universally true.

There are instances wherein applied research is conducted as following other applied research; and, therein may be inherently distant from basic research at that point. Without further clarification of what constitutes “severable” and how close the applied research must be to the basic research, the public is left to guess what is intended here.

- Second, the phrase and following enumeration of “*technology, materials, processes, methods, devices, or techniques*” could become restrictive as only the word “technology” is presently defined in the EAR.
- Third, the presence of “and” prior to the phrase “attempts to advance the state of the art” is greatly problematic. A standard practice within the fundamental research community is to reproduce prior art to validate other researchers’ results, often using alternate techniques. As such, this kind of applied research might not necessarily attempt to “advance the state of the art.”

The IEEE-USA suggests using the NSF definition for both “basic” and “applied” research and retaining some specific reference to those definitions within the description of what constitutes fundamental research.

Deletion of the Clarifications and Questions and Answers

IEEE-USA is concerned about the proposal to delete clarifying questions and answers that address the definition of “Publicly Available Information” and “Technology and Software Subject to the EAR” in EAR 734 Supplement 1. The answers offer clarifications that are necessary to avoid misinterpretation of the EAR. While we understand the intention of the answers is to afford the public with illustrative examples instead of serving a regulatory purpose, from the perspective however, from the perspective of academia and industry, the presence of the answers within the regulations does serve as legally-binding guidance, whereas a website which may be less frequently visited is – in general – not legally-binding. Thus, we recommend maintaining the presence of the answers to prior questions that have relevancy under the proposed rules.

Thank you for giving us the opportunity to provide this information. Feel free to contact IEEE-USA’s Director of Government Relations, Mr. Russell Harrison, at r.t.harrison@ieee.org for further assistance.

Respectfully submitted,



James A. Jefferies
President, IEEE-USA

3 August 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Via Email: publiccomments@bis.doc.gov

ATTN: RIN 0694-AG32 Revisions to Definitions in the Export Administration Regulations (80 Fed. Reg. 31505)

To Whom It May Concern:

BAE Systems plc offer the following comments in response to the request from the Bureau of Industry and Security (BIS) on June 3, 2015 (80 Fed. Reg. 31505). BAE Systems appreciates this outreach from BIS to industry and would like to take this opportunity to provide its comments to the proposed rule.

- 1) **Overview.** As a non-US defense industry participant in Europe, BAE Systems greatly appreciates BIS's efforts to clarify and update certain regulations related to the definitions of release, technology, and the use of encryption for the transmission of technology and software. We are largely supportive of the proposed rules, but would propose certain changes and clarification based on our experience.
- 2) **Release.** Under the proposed new EAR §734.15, we support the clarification of the definition of "release" so that a release only occurs when a physical, aural, or tactile inspection actually *reveals* controlled technology or source code. We understand that briefly seeing an item, such as during a plant tour, would not be sufficient to constitute a release of technology in most cases. We welcome the clarification offered by this new definition.
- 3) **Use of Encryption** – We are largely supportive of the proposed addition of the list of activities that are not exports, reexports, or retransfers under the EAR (§734.18). We believe that the use of secure methods of communicating technology and software should be encouraged and welcome the establishment of an agreed baseline for such encryption standards. However, we believe these proposed rules should be modified or clarified to address several key points.
 - a. BIS should clarify that emails transiting a nation's internet infrastructure are not "stored" in such a country. The proposed addition of EAR §734.18(a)(4)(iv) includes a restriction that the unclassified technology or software cannot be "stored" in the Russian Federation or any country listed in Country Group D:5. However, the term "stored" is not defined. One would assume that this means intentional storing of information on a data server for a period of time rather than an email transiting a server and being retained temporarily for this purpose. We urge BIS to clarify that

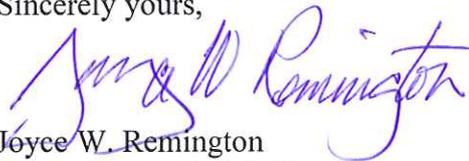
these country restrictions only apply to ongoing storage and not the possible transit of emails through those countries. This clarification is necessary as the sender of a secured email typically has no control over what countries an email passes through on its way to its final destination – even emails sent between a sender and receiver in the United States may transit a third country.

- b. Encrypted items in storage should not be considered a violation where transferred to restricted destinations without a party's knowledge. The revised EAR §734.18(a)(4)(iv) should address the scenario where properly encrypted data or software stored on a third-party's server, such as a cloud server, is transferred from a permitted sender to a restricted jurisdiction without the permission or knowledge of the company utilizing the third party's service. As such, we suggest adding a "knowingly" standard to protect those entities that conducted due diligence in procuring third-party services from providers that do not store technology or software in a prohibited country but whose data may end up in one of those countries without their prior knowledge or consent.
- c. The proposed EAR §764.2(l) states that the unauthorized release of decryption keys, network access codes, passwords, or other transfer information that would allow access to the encrypted information in clear text is an export control violation. In order to avoid any duplication of licensing, we ask that BIS clarify that existing authorizations for the export, reexport, or retransfer of information also authorize the release of decryption keys, network access codes, passwords, or other transfer information that would give access to that same controlled information to authorized parties on export license approvals. Without this clarification, companies may need to seek two separate authorizations: one that covers the export, reexport, or retransfer of controlled information, and one that covers the release of decryption keys, network access codes, passwords, or other transfer information to the same authorized parties.

We hope that you will consider these alternative recommendations in the final regulation.

Thank you for your consideration of our comments.

Sincerely yours,



Joyce W. Remington
Group Deputy Head of Export Control, Licensing &
Policy



August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave., NW
Washington, DC 20230

Submitted via Email to: publiccomments@bis.doc.gov

RE: RIN 0694-AG32

Dear Ms. Hess,

The Johns Hopkins University (JHU) works with the Council on Governmental Relations (COGR) and the Association of American Universities (AAU). Its Export Control Officer is a member of the Association of University Export Control Officers (AUECO). We have reviewed these organizations' comments in response to the Bureau of Industry and Security's (BIS) RIN 0694-AG32 (*Revisions to Definitions in the Export Administration Regulations*) and in support offer our own, supplementary comments below.

We appreciate the progress that has been made by BIS and DDTC in creating more consistent and clear export control regulations, as well as their willingness to consider the impact of existing and proposed regulations upon U.S. universities. We know quite well that it can be exceedingly difficult to find an acceptable compromise between preserving the freedoms and openness prized by many U.S. institutions and reining in the same freedoms/openness in order to protect national security.

Fundamental Research Definitions

"Non-proprietary": Effective export control compliance practices at JHU's academic divisions require clear rules and definitions associated with fundamental research. We are satisfied with the proposed use of a definition of fundamental research found in NSDD-189. We are also not fundamentally opposed to the suggested, "simpler definition," although we expect that many will require guidance as to the appropriate interpretation of the term "non-proprietary."

"Basic Research" and "Applied Research": In order to accurately and consistently identify its research as "fundamental," JHU relies heavily upon a shared understanding of what "basic research" and "applied research" typically look like, as well as an ability to differentiate fundamental research from the "development" of items that are based upon concepts first spawned by basic research and later refined and validated by applied research. We have no objection to the continued use of the definition of basic research currently found at EAR 772.1. As for the definition of applied research, we are also not opposed to the use of language taken from OMB Circular A-11 but nevertheless prefer the language drawn from the Defense Federal Acquisition Regulation Supplement (specifically, DFARS 48 CFR part 31.205-18), so long as it includes the paragraph from that section that begins with, "*Applied research is not... .*" The additional language should help to mark the boundary between activities

Office of the Provost

265 Garland Hall 3400 N. Charles Street Baltimore, MD 21218 410-516-8070 <http://web.jhu.edu/administration/provost>



involving the assessment and refinement of basic research discoveries (“applied research”) and those subsequent activities involving the practical application of concepts validated by applied research (“development”).

Controls on Fundamental Research Inputs: We appreciate the clarity introduced by proposed Note 1 to Paragraph (a) of EAR Section 734.8. JHU’s export control compliance program has historically assumed that the information, equipment, or software used to conduct its fundamental research may *not* necessarily be excluded from export controls. In fact, a large proportion of our export compliance screening effort is rooted in this assumption, as it is exceptionally difficult to anticipate and screen all inputs that may occur, especially when we are working with collaborators who may be unable or unwilling to identify the restricted status of what they are offering to us in support of our research. Notwithstanding our assumptions and current practice, we think it would be helpful if BIS were to make clear to the university community how this proposed Note is consistent with the NSDD-189’s hands-off approach to the “conduct” of federally –funded fundamental research.

Software as Fundamental Research “Result”: We note that proposed EAR Section 734.3(b)(ii) refers to “information and ‘software’ ” that arise during, or result from, fundamental research but that the Section to which it refers (734.8) only mentions “technology.” As with other universities, we are concerned that this could mean that that BIS will no longer consider software to be a type of fundamental research “result” of the sort that is included in the NSDD-189’s definition of fundamental research. If that is the case, then we believe that this would introduce counterproductive restrictions upon the dissemination of the results of applied research. It makes more sense to us that, perhaps at a later stage of activity, the validated software outputs of applied research may be incorporated into software *development* activity that would warrant the imposition of EAR export control upon items developed. Thus, we suggest that software arising during, or resulting from, fundamental research continue to be excluded from EAR controls.

Educational Information

We support the suggestion made by other universities and organizations that BIS revise proposed EAR Section 734.3(b)(3)(iii) such that it makes clear that, in addition to general, commonly taught principles, new discoveries will also be included among the type of “educational” items that may be incorporated into existing or new catalog courses or teaching laboratories and that they will not be subject to the EAR. This would make less likely a narrow interpretation of the section that could stifle the dissemination of information needed to educate and train students to enter a competitive job market. As an alternative, we support MIT’s suggestion that the Section be shortened to read simply as, “(iii) Released by instruction in a catalog course or associated teaching laboratory of an academic institution.”

Q&A: Supplement No. 1 to Part 734

Please continue to publish the questions and answers found in Supplement No. 1 to part 734. We acknowledge that offering such a section can create an expectation that it be continually updated – requiring resources that may be in short supply – but we believe that maintaining it promotes consistency in interpretation and likely reduces the overall volume of requests for guidance that is directed to your licensing division.

Office of the Provost

265 Garland Hall 3400 N. Charles Street Baltimore, MD 21218 410-516-8070 <http://web.jhu.edu/administration/provost>



Effective Date of Final Rule

JHU's export control compliance practices are dependent upon the sharing of knowledge with – and delegation of responsibility to – a very large population of faculty, administrators and staff. Depending upon the content of the final rule, it could easily take several months for us to be reasonably confident that compliance practices have been modified in accord with the regulatory changes. We note that changes to the EAR have in the past been accompanied by effective-date delays of up to six months and urge BIS to allow at least this much time for us to recalibrate our practices accordingly.

Thank you for providing JHU with an opportunity to offer its comments on these proposed changes to the Export Administration Regulations.

Sincerely,

A handwritten signature in black ink, appearing to read "DW" or similar initials.

Denis Wirtz

Vice Provost for Research, Johns Hopkins University
Theophilus H. Smoot Professor in Engineering Science
Departments of Chemical and Biomolecular Engineering, Oncology and Pathology
Director, Johns Hopkins Physical Sciences in Oncology Center
Associate Director, Johns Hopkins Institute for NanoBioTechnology
Director, NCI postdoctoral training program
Director, NCI predoctoral training program
Johns Hopkins University

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY
244 WOOD STREET
LEXINGTON, MASSACHUSETTS 02420-9108

3 August 2015

U.S. Department of Commerce
Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
Washington, DC 20230

RE: RIN 0694-AG32 “Revisions to Definitions in the Export Administration Regulations”

MIT Lincoln Laboratory (“MIT LL”), a Federally Funded Research and Development Center (“FFRDC”) operated by the Massachusetts Institute of Technology (“MIT”), appreciates the opportunity to comment in response to the Bureau of Industry and Security (BIS) RIN 0694-AG32, *Revisions to Definitions in the Export Administration Regulations*.

The proposed revisions, as well as the State Department’s own offering under RIN 1400-AD70 regarding ITAR definitions, represent significant progress towards harmonized and constructive definitions of terms. However, certain proposed definitions would significantly affect the ability of U.S. universities, as well as the FFRDCs and/or University-Affiliated Research Centers (“UARCs”) they may operate, to achieve their missions and maintain U.S. leadership in education and research. In the case of MIT, and MIT LL in particular where almost all research is U.S. government funded, the impact of these proposed revisions would affect the missions of our myriad U.S. government sponsors as well.

While MIT will submit a response that addresses aspects of the proposed revisions of interest to all of the departments/laboratories that comprise the Institute (including MIT LL), the intent of the following comments is to emphasize and provide an additional perspective on those of particular interest to MIT LL.

“Fundamental Research”

Proposed Alternative Definition

MIT LL welcomes BIS’s proposed alternate definition of “fundamental research”, which increases clarity while remaining consistent with NSDD-189: “Fundamental research’ means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.” Our only concern is the undefined term

“non-proprietary.” MIT LL proposes a minor revision: “‘Fundamental research’ means research in science and engineering, the results of which ordinarily are published and shared broadly within

the scientific community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.” This definition captures the intent of BIS in clear, unambiguous language.

If the proposed alternate definition is adopted, it will not be necessary to define “basic research” and “applied research,” which will be subsumed by “fundamental research”. These terms have led to uncertainty since there are multiple definitions in different areas of federal regulations; even with a single agreed definition, differing judgments are common. As MIT LL is at times a performer, but more frequently a funding “sponsor” (via subcontracts) of fundamental research, the proposed alternate definition is a welcome, commonsense revision.

Finally, the removal of “basic and applied research” from this definition appears to be more consistent with the spirit of the “Fundamental Research” memo issued in 2010 by then Under Secretary of Defense for Acquisition, Technology and Logistics Ashton B. Carter. While issued by DoD, and therefore perhaps of greater import to “fundamental research” as defined under the ITAR, it nonetheless serves as a U.S. government precedent for a more expansive view of “fundamental research.”

The “Carter Memo,” which reinforces earlier guidance and “deals explicitly with additional facets of fundamental research,” expanded the types of DoD funding, beyond traditional “basic research” and “applied research” funding, that could be used to perform research free from restrictions on publications or personnel. While the “Carter Memo” does not explicitly state that unrestricted research performed with “other Budget Activities” is “fundamental research,” it appears to portend that in spirit it should be considered as such.

“Fundamental research”, “technology”, and “software”

“Software” and fundamental research: The current §734.3(b)(3) states that “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR. Under the proposed §734.8(a), only “‘technology’ that arises during, or results from, fundamental research and is ‘intended to be published’” would not be subject to the EAR.

While the amount of “fundamental research” performed by MIT LL is small in comparison to the amount of controlled research performed for our U.S. government sponsors, much of our fundamental research involves collaborations with universities, including MIT. This change would significantly complicate and restrict our ability to engage in fundamental research with university partners: while natural-language documents written by a researcher would be “technology” that could be freely shared as arising during fundamental research, a computer-language document written by the same researcher, working on the same project (a program in source code), would be subject to deemed export restrictions. Additionally, for much of this fundamental research, the “result” of greatest interest to our U.S. government sponsors is the

software itself. “Software” resulting from university research is “published” as well as “technology,” as recognized in the current §734.7(b). The export definitions in §734.2(b) recognize the similarities between software and technology.

MIT LL strongly recommends that software arising during, or resulting from, fundamental research should not be subject to the EAR.

End-to-End Encryption Standard

MIT LL welcomes the addition of §734.18 listing activities that are not exports, reexports or transfers, in particular, the exclusion of sending, taking or storing software that is secured using end-to-end encryption from export activities. This will enable MIT LL to take greater advantage of commercial cloud storage/hosting for certain research activities. While the convenience of cloud storage/hosting has made it the preferred means of storage/hosting for many of our U.S. government sponsors, MIT LL has been reluctant to avail itself of such services due to export compliance concerns. The addition of §734.18 will greatly benefit both MIT LL and our U.S. government sponsors.

Questions and Answers - Technology and Software Subject to the EAR

MIT LL finds the questions and answers provided in Supplement No. 1 to part 734 in the regulations highly useful and urges BIS to retain this section. While we agree that the questions and answers are illustrative, inclusion of them in the EAR removes the uncertainty created by changes due to interpretive differences without benefit of the rulemaking process. We are concerned that removal of the questions and answers, which we use to guide export control decisions when interacting or considering interacting with universities, would create increased uncertainty in our application of key concepts.

Effective Date of the Final Rule

Although RIN 0694-AG32 and the accompanying RIN 1400-AD70 do not alter the CCL or USML, they would have a significant impact on MIT LL’s export compliance program, particularly as it relates to collaborations with university partners. While only a small portion of our many ongoing research activities involve university partners, the benefits of these collaborations, which enable MIT LL and our U.S. government sponsors to work with some of the brightest minds in their respective fields, are disproportionately large and worthy of preserving. Ensuring that collaborations with university partners alone will be compliant with the final rules (we assume both would take effect concurrently) will represent a significant regulatory burden.

MIT LL suggests at minimum a 6-month delay in the effective date, and further that the revised regulations be applicable only to new sponsored research begun after the effective date of the Final Rule.

Thank you for the opportunity to provide comments on RIN 0694-AG32. If you have any questions or require additional information, do not hesitate to contact me at 781-981-5997, zsweet@ll.mit.edu.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Zach Sweet', with a stylized flourish at the end.

Zach Sweet
Export Compliance Officer



Perry A Smith
Director
Export and Import Compliance
Office of the General Counsel

**Rockwell
Collins**

400 Collins Road NE
Cedar Rapids, IA 52498
319.295.5396 Fax 319.295.8909
perry.smith@rockwellcollins.com

August 3, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security

Re: Comments Related to Revision of 15 CFR Parts 734, 740, 750, 764 and 772.

Dear Ms. Hess:

Rockwell Collins appreciates the opportunity to provide comments on the proposed Amendment to the Export Administration Regulations: Revision of 15 CFR Parts 734, 740, 750, 764 and 772; (RIN 0694-AG32), published in the Federal Register on June 3, 2015.

Rockwell Collins, Inc. is an industry recognized leader in the design, production and support of communications and aviation electronics for commercial and military customers worldwide. While our products and systems are primarily focused on aviation applications, our Government Systems business also offers products and systems for ground and shipboard applications. The integrated system solutions and products we provide to our served markets are oriented around a set of core competencies: communications, navigation, automated flight control, displays/surveillance, simulation and training, integrated electronics and information management systems. We also provide a wide range of services and support to our customers through a worldwide network of service centers, including equipment repair and overhaul, service parts, field service engineering, training, technical information services and aftermarket used equipment sales. We are headquartered at 400 Collins RD NE, Cedar Rapids, Iowa 52498 and employ approximately 20,000 individuals worldwide.

Regarding the proposed changes to the International Traffic in Arms Regulations: Revision of 15 CFR Parts 734, 740, 750, 764 and 772: Amendment to the Export Administration Regulations: **Revisions to Definitions in the Export Administration Regulations.**

Rockwell Collins submits the following Comments:

§ 734.7 Published.

(a) Except as set forth in paragraph (b) of this section, unclassified "technology" or "software" is "published," and is thus not "technology" or "software" subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination such as through any of the following:

- (1) Subscriptions available without restriction to any individual who desires to obtain or purchase the published information;
- (2) Libraries or other public collections that are open and available to the public, and from which the public can obtain tangible or intangible documents;
- (3) Unlimited distribution at a conference, meeting, seminar, trade show, or exhibition, generally accessible to the interested public;
- (4) Public dissemination (*i.e.*, unlimited distribution) in any form (*e.g.*, not necessarily in published form), including posting on the Internet on sites available to the public; or
- (5) Submission of a written composition, manuscript or presentation to domestic or foreign coauthors, editors, or reviewers of journals, magazines, newspapers or trade publications, or to organizers of open conferences or other open gatherings, with the intention that the compositions, manuscripts, or publications will be made publicly available if accepted for publication or presentation.

Ms. Hillary Hess

August 3, 2015

Re: Comments Related to Revision of 15 CFR Parts 734, 740, 750, 764 and 772.

Page 2 of 6

(b) Published encryption software classified under ECCN 5D002 remains subject to the EAR unless it is publicly available encryption object code software classified under ECCN 5D002 and the corresponding source code meets the criteria specified in § 740.13(e) of the EAR.

COMMENTS:

1. *As written this regulation suggests that releasing (publishing) technology that is unclassified but subject to the EAR makes that technology no longer subject to the EAR. For example: publishing a YouTube video describing how to operate and/or repair a weather radar, which is technology subject to the EAR under 6E991 would no longer be subject to the EAR after publishing. This would also include 3E611, 7E101, 7E004.7 and all other unclassified technology.*

§ 734.18 Activities that are not exports, reexports, or transfers.

(a) The following activities are not exports, reexports, or transfers:

(1) Launching a spacecraft, launch vehicle, payload, or other item into space.

(2) While in the United States, releasing technology or software to United States citizens, persons lawfully admitted for permanent residence in the United States, or persons who are protected individuals under the Immigration and Naturalization Act (8 U.S.C. 1324b(a)(3)).

(3) Shipping, moving, or transferring items between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, or the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census.

(4) Sending, taking, or storing technology or software that is:

(i) Unclassified;

(ii) Secured using end-to-end encryption;

(iii) Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and

(iv) Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation.

(b) *Definitions.* For purposes of this section, 'end-to-end encryption' means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

(c) The ability to access "technology" or "software" in encrypted form that satisfies the criteria set forth in paragraph (a)(4) of this section does not constitute the release or export of such "technology" or "software."

Note to § 734.18: Releasing “technology” or “software” to any person with knowledge that a violation will occur is prohibited by § 736.2(b)(10) of the EAR.

COMMENTS:

1. *Rockwell Collins suggests that the language in (4)(iii) mirror the language in the ITAR § 120.52(a)(4)(iii) defining the use of the Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications.*

Use of alternative methods of encryption outside of the NIST/FIPS 140-2 standards can and will cause interoperability issues across industry. It is recommended that alternative methods not be allowed to cause industry to adopt the NIST/FIPS standard. It is recommended that “or other similarly effective cryptographic means;” be removed.

2. *It is recommended that a transition period be provided to allow industry time to modify its IT systems to accommodate and deploy end-to-end encryption that is compliant with the NIST/FIPS 140-2 standard.*

PART 750—APPLICATION PROCESSING, ISSUANCE, AND DENIAL

§ 750.7 Issuance of licenses.

(a) *Scope.* Unless limited by a condition set out in a license, the export, reexport, or transfer (in-country) authorized by a license is for the item(s), end-use(s), and parties described in the license application and any letters of explanation. The applicant must inform the other parties identified on the license, such as the ultimate consignees and end users, of the license’s scope and of the specific conditions applicable to them. BIS grants licenses in reliance on representations the applicant made in or submitted in connection with the license application, letters of explanation, and other documents submitted. A BIS license authorizing the release of technology to an entity also authorizes the release of the same technology to the entity’s foreign nationals who are permanent and regular employees (and who are not proscribed persons under U.S. law) of the entity’s facility or facilities authorized on the license, except to the extent a license condition limits or prohibits the release of the technology to nationals of specific countries or country groups.

COMMENTS:

1. *As written the scope of a license approval could be misconstrued to assume that the approved license also includes the item(s), end-use(s) and parties not included in a license application but included in supporting documentation. It is recommended the language be written as follows:*

“Unless limited by a condition set out in a license, the export, reexport, or retransfer (in-country) authorized by a license is for the item(s), end-use(s), and parties described in the license application.” Remove the words “and any letters of explanation”.

PART 772—DEFINITIONS OF TERMS

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

Applied research. See § 734.8(c) of the EAR.

Basic scientific research. (GTN)— Experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective. See also § 734.8(c) of the EAR.

Ms. Hillary Hess

August 3, 2015

Re: Comments Related to Revision of 15 CFR Parts 734, 740, 750, 764 and 772.

Page 4 of 6

Export. See § 734.13 of the EAR.

Fundamental research. See § 734.8 of the EAR.

Peculiarly responsible. An item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions” if it is used in or for use in the “development,” “production,” “use,” operation, installation, maintenance, repair, overhaul, or refurbishing of an item subject to the EAR unless:

- (1) The Department of Commerce has determined otherwise in a commodity classification determination;
- (2) [Reserved];
- (3) It is identical to information used in or with a commodity or software that:
 - (i) Is or was in production (*i.e.*, not in development); and
 - (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
- (4) It was or is being developed with “knowledge” that it would be for use in or with commodities or software:
 - (i) Described in an ECCN; and
 - (ii) Also commodities or software either not enumerated on the CCL or the USML (*e.g.*, EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
- (5) It was or is being developed for use in or with general purpose commodities or software, *i.e.*, with no “knowledge” that it would be for use in or with a particular commodity or type of commodity; or
- (6) It was or is being developed with “knowledge” that it would be for use in or with commodities or software described:
 - (i) In an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or
 - (ii) Exclusively for use in or with EAR99 commodities or software.

Proscribed person. A person who is prohibited from receiving the items at issue or participating in a transaction that is subject to the EAR without authorization by virtue of U.S. law, such as persons on the Entity List, Specially Designated Nationals, or debarred parties.

Publicly available encryption software. See § 740.13(e) of the EAR.

Published. See § 734.7 of the EAR.

Reexport. See § 734.14 of the EAR.

Release. See § 734.15 of the EAR.

Required. (General Technology Note)—As applied to “technology” or “software”, refers to only that portion of “technology” or “software” which is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics or functions. Such “required” “technology” or “software” may be shared by different products. For example, assume product “X” is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D”, and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Note 1 to the definition of *required*: The references to “characteristics” and “functions” are not limited to entries on the CCL that use specific technical parameters to describe the scope of what is controlled. The “characteristics” and “functions” of an item listed are, absent a specific regulatory definition, a standard dictionary’s definition of the item. For example, ECCN 9A610.a controls “military aircraft specially designed for a military use that are not enumerated in USML paragraph VIII(a).” No performance level is identified in the entry, but the control characteristic of the aircraft is that it is specially designed “for military use.” Thus, any technology, regardless of significance, peculiar to making an aircraft “for military use” as opposed to, for example, an aircraft controlled under ECCN 9A991.a, would be technical data “required” for an aircraft specially designed for military use thus controlled under ECCN 9E610.

Note 2 to the definition of *required*: The ITAR and the EAR often divide within each set of regulations or between each set of regulations:

1. Controls on parts, components, accessories, attachments, and software; and
2. Controls on the end items, systems, equipment, or other items into which those parts, components, accessories, attachments, and software are to be installed or incorporated. Moreover, with the exception of technical data specifically enumerated on the USML, the jurisdictional status of unclassified technical data or "technology" is the same as the jurisdictional status of the defense article or "item subject to the EAR" to which it is directly related. Thus, if technology is directly related to the production of a 9A610.x aircraft component that is to be integrated or installed in a USML VIII(a) aircraft, then the technology is controlled under ECCN 9E610, not USML VIII(i).

"Technology" means: (a) Except as set forth in paragraph (b) of this definition:

- (1) Information necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control "technology") of an item. "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information gleaned through visual inspection;

Note to paragraph (a)(1) of this definition:

The modification of an existing item creates a new item and technology for the modification is technical data for the development of the new item.

- (2) [Reserved];
- (3) [Reserved];
- (4) [Reserved]; or
- (5) Information, such as decryption keys, network access codes, or passwords, that would allow access to other "technology" in clear text or "software."

(b) "Technology" does not include:

- (1) Non-proprietary general system descriptions;
- (2) Information on basic function or purpose of an item; or
- (3) Telemetry data as defined in note 2 to Category 9, Product Group E (see Supplement No. 1 to Part 774 of the EAR).

Transfer. A shipment, transmission, or release of items subject to the EAR either within the United States or outside the United States. *For in country transfer/transfer (in-country)*, see § 734.16 of the EAR.

Note to definition of *transfer*: This definition of "transfer" does not apply to § 750.10 of the EAR or Supplement No. 8 to part 760 of the EAR. The term "transfer" may also be included on licenses issued by BIS. In that regard, the changes that can be made to a BIS license are the non-material changes described in § 750.7(c) of the EAR. Any other change to a BIS license without authorization is a violation of the EAR. See §§ 750.7(c) and 764.2(e) of the EAR.

Comments:

1. *In reference to the definition of "Technology", (a)(5) Rockwell Collins does not agree that decryption keys, network access codes or passwords, that would allow access to other "technology" in clear text or "software", should be considered technology. Such are not specifically enumerated within the CCL. While it is recognized the keys, access codes and passwords control access to other technology or software (both encrypted and unencrypted), such should not be controlled as technology requiring authorization to export.*
2. *For the Definition of "Technology" suggest adding to (b)(4) "information that is subject to the EAR but published without restriction on further dissemination".*
3. *Suggest the expansion of (b)(2) to include the phrase "including requirements that do not contain design implementation information"*

Ms. Hillary Hess

August 3, 2015

Re: Comments Related to Revision of 15 CFR Parts 734, 740, 750, 764 and 772.

Page 6 of 6

Rockwell Collins is fully committed to supporting the Administration's efforts in moving export control reform forward. We greatly appreciate the opportunity to provide comments to the proposed changes.

If you have any questions or would like to discuss the comments provided above, feel free to contact me directly at 319-295-5396, or via email at perry.smith@rockwellcollins.com

Sincerely,



Perry A. Smith
Director, Export and Import Compliance
Rockwell Collins



TEXAS TECH UNIVERSITY™

Office of the President

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I am writing on behalf of Texas Tech University, an institution of higher education of the State of Texas. Texas Tech University (TTU) is providing the following comments in response to the Bureau of Industry and Security RIN 0694-AG32 *Revisions to Definitions in the Export Administration Regulations (EAR)*. TTU supports revisions to the EAR that clarify and harmonize definitions with the International Traffic in Arms Regulations.

We appreciate the opportunity to comment on the harmonized definitions and believe they are an important step forward. They advance meaningful export control reform and contain many helpful changes and clarifications (e.g. redefinition of "release," clarification that submission of manuscripts to journal editors constitutes "published" information). The changes will have significant impact on our university. Below are our comments in response to the eight issues on which BIS has requested specific comments:

1. Whether the proposed revisions create gaps, overlaps, or contradictions between the EAR and the ITAR, or among various provisions within the EAR.

Response: Most inconsistencies between the EAR and ITAR are either relatively minor or reflect longstanding practices. There is a major conflict, however, between the proposed EAR and ITAR definitions in their treatment of prepublication review (to assure that publication does not divulge a sponsor's proprietary information). EAR 734.8(b) continues to provide that such review does not change the status of technology. Technology that arises during or results from fundamental research is still "intended to be published" when prepublication review is conducted to ensure patent rights are not compromised and when there is only a temporary delay in publication of the research results. In contrast, ITAR 120.49 states that technical data that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the technical

data without *any restriction or delay*, including temporary delays for research sponsor proprietary information review. (Emphasis added.)

TTU strongly opposes the proposed ITAR interpretation that would exclude any research subject to prepublication review from being considered fundamental research, even when the results will be published. It is reasonable, and our current practice, to allow industrial sponsors time to review proposed publications and file provisional patents prior to publication, which usually occurs with a maximum 90-day delay. The proposed ITAR provision will remove any research projects involving defense articles subject to such review from fundamental research. No explanation is provided as to the reason for the different policies. We urge that the ITAR be aligned with the EAR interpretation and definition of fundamental research.

Also inconsistent with the ITAR are the provisions related to government-sponsored research covered by contract controls in EAR 734.11. The proposed EAR rule essentially restates the current 734.11(a), which universities have found confusing. We join our colleagues at other universities in requesting instead the ITAR language at 120.49(b) Note 3, modified to apply to technology arising during or resulting from fundamental research. The examples in 734.11(b) are helpful and TTU requests they be retained.

One change that is important to educational institutions is the proposed restatement of the "education exemption" in the current EAR 734.9, which is removed. The new statement in the proposed EAR 734.3(b)(3)(iii) merges current ITAR (120.10(b)) and EAR text to state "information and software that . . . concern general scientific, mathematical, or engineering principles commonly taught in schools, and released by instruction in a catalog course or associated teaching laboratory of an academic institution." If narrowly interpreted, the revised 743.3(b)(3)(iii) would inhibit the ability of TTU to develop new courses in emerging areas of science and engineering critical to the employability of its graduates and their future competitiveness in the industrial sector. We suggest that the "and" be changed to "or" to avoid unintentionally limiting this section, i.e. to clearly cover a new university course in a technology area so long as it is included in a course catalog.

2. Whether the alternative definition of fundamental research suggested in the preamble should be adopted.

Response: The proposed alternative definition would read: "Fundamental research means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." While this definition is shorter, there may be some vagueness in the term "non-proprietary." The proposed ITAR rule discussed above demonstrates confusion about what constitutes non-proprietary research. We urge significant caution in changing a definition of fundamental research that has been endorsed by White House Administrations of both parties over the years and that has served the scientific community well.

Research findings in the form of technology and software arising during or resulting from fundamental research, intended to be published, and should not be subject to EAR. Currently the EAR §734.3(b)(3) states that "publicly available technology and software "[that] arise during, or result from, fundamental research" are not subject to the EAR. The proposed 734.3(b) (3) and 734.7(a) also treat technology and software similarly. Under the proposed §734.8(a), "technology" that arises during, or results from, fundamental research and is 'intended to be published'" would not be subject to the EAR, but software is not mentioned. "Software" should be included as well as "technology."

Research findings resulting from fundamental research may be written in natural-language or computer language. In either case it is "technology" that should be able to be freely shared as arising during or resulting from fundamental research. No explanation is provided as to the reason for changing the recognition of the similarities between software and technology in the current EAR (734.2(b); 734.7(b)). This change would significantly complicate and restrict university research; while natural-language documents written by a researcher would be "technology" that could be freely shared as arising during fundamental research, a computer-language document (a program in source code) written by the same researcher would be subject to deemed export restrictions. TTU strongly recommends that software arising during, or resulting from, fundamental research should not be subject to the EAR.

The current presumption in EAR 734.8(b) that university-based research will be considered fundamental research appears to have been eliminated. There is no clear policy reason stated for this change. The applicability should continue to be determined by the other criteria in 734.8(b). We urge BIS to restate the presumption in the final rule.

3. Whether the alternative definition of applied research suggested in the preamble should be adopted, or whether basic and applied research definitions are needed given that they are subsumed by fundamental research.

Response: The EAR changes include definitions of "basic research" (734.8, currently found at EAR 772.1) and "applied research" (currently found in the DFARS). The preamble suggests that the DFARS definition be used, which is reflected in the ITAR (120.49). It also suggests an alternate definition of applied research taken from OMB Circular A-11: "Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met." This definition is well-understood by universities in the context of reporting federal expenditures to NSF, and we suggest that it be adopted.

If the DFARS definition is adopted instead, the definition of "applied research" would be clarified by including the rest of 48 CFR part 31.205-18: "Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development, defined in this subsection." The "for sale" criterion will help to distinguish between "applied research" and "development" activities.

4. Whether the questions and answers in existing Supplement no. 1 to part 734 proposed to be removed (to the BIS website) have criteria that should be retained in part 734.

Response: The Q&As are very helpful. If they are removed from the EAR and placed on the website, they will no longer have the same regulatory weight. We also note that supplements to other parts of the EAR contain important regulatory information (e.g. Supplement No. 1 to Part 740). We request that the Q&As be retained in part 734.

5. With respect to end-to-end encryption as described in the proposed rule (sec. 734.18), whether the illustrative standard in the proposed EAR rule also should be adopted in the ITAR; whether the safe harbor standard in the proposed ITAR rule also should be adopted in the EAR, or whether the two bodies of regulations should have different standards.

Response: We appreciate that the proposed rules address cloud computing situations, which have been an area of considerable uncertainty under the current rules. We prefer the proposed EAR definition in 734.13(a)(6), which requires knowledge that releasing information relating to encryption will cause or permit the transfer of technology to a foreign national. In general, we believe that knowledge or intent to transfer controlled information should be required for an "export" or "deemed export" to occur. The addition of 734.18 listing activities that are not exports, re-exports or transfers is a useful addition to the EAR. In particular, the exclusion of sending, taking or storing software that is secured using end-to-end encryption from export activities is welcome as it will reduce the faculty burden associated with international travel and the need to monitor and conduct research using main campus resources while abroad. We also prefer the EAR provision in 734.18(4)(iii) providing for "other similarly effective cryptographic means" for securing technology or software.

The restriction in 734.18(a)(4)(iv) to countries not listed in Country Group D:5 unfortunately may substantially limit the usefulness of the proposed rule. Most cloud providers insist on storing data anywhere that they want. We suggest BIS consider adding a note that a contract that imposes these obligations on a vendor is sufficient for compliance purposes, to provide a greater safe harbor. Ensuring actual compliance is beyond a university's control.

6. Whether encryption standards adequately address data storage and transmission issues.

Response: TTU favors the proposed hardware or software compliant with Federal Information Processing Standards Publication 140-2 supplemented in accordance with NIST guidance or other similarly effective means.

7. Whether the proposed definition of "peculiarly responsible" effectively explains how items may be "required" or "specially designed" for particular functions.

Response: The definitions provide appropriate explanations.

8. The effective date of the final rule.

Response: TTU supports a six-month delayed effective date. If the proposed changes to ITAR 120.49(b) Prepublication Review go to the final rule without changes, TTU will need to significantly change our sponsored research practices associated with review and negotiation of industry sponsored research agreements. A review will be required of current and ongoing projects. We will time to develop new procedures determining when ITAR applies to fundamental research with prepublication review. Staff will need to implement additional technology control plans, monitor those plans, and establish procedures to remove the plans once prepublication review has occurred. In addition, TTU will need to submit license applications for foreign national students who are participating in affected research. Export compliance training will be required for additional departments on campus.

These procedures will likely require additional staffing for export compliance. TTU will not be able to meet the compliance obligations imposed by the addition of prepublication review language within 30 days of publication of the rules. Our view is that significant changes in definitions should have as long a lead time as possible for implementation. Therefore we support a six-month delayed effective date.

Conclusion

In closing, we again want to express our appreciation to BIS for your willingness to engage universities in dialogue on these issues. We believe the EAR changes are mostly positive and deserving of support. We hope BIS will consider our comments in finalizing the proposed definitions, and are available to provide more information or discuss these matters further.

Sincerely,

A handwritten signature in black ink, appearing to read "M. Duane Nellis". The signature is fluid and cursive, with a distinct flourish at the end.

M. Duane Nellis, Ph.D.
President

July 31, 2015

VIA EMAIL TO publiccomments@bis.doc.gov

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.

RE: Revisions to Definitions in the Export Administration Regulations
(RIN 0694-AG32)

Dear Ms. Hess:

Vanderbilt University welcomes the opportunity to comment on the proposed revisions to the EAR. We appreciate and support the joint efforts of the Departments of State, Commerce, and Defense to reform and harmonize U.S. Export Control Regulations. While Vanderbilt views the proposed EAR amendment as a positive, important step forward, some of the revisions to the definitions are problematic.

Software. The revision that concerns us most is the proposed change that would expose software arising from university research to the EAR. The confusion in the proposed revision stems from the wording of the draft, which omits software, and states in the preamble that software is not technology arising from fundamental research. We respectfully disagree. Software is the means of adapting the functions of complex systems to the environment and users, and Vanderbilt researchers pursue significant fundamental research interests in the exploration of theoretical foundations, modeling, design, and software engineering. In many projects for government agencies and corporate sponsors, developing software is the objective of the research. Whether the output of fundamental research is a natural language publication, program, application, or algorithm should not matter when deciding whether or not it is subject to the EAR.

These comments are intended to address the key issues impacting Vanderbilt. We are a member of the Association of American Universities and Council on Governmental Regulations, and we concur with the comments being submitted by these organizations with respect to the proposed revisions generally. We also support the comments being submitted by the Association of University Export Control Officers regarding these proposed revisions.

Sincerely,



Timothy P. McNamara
Vice Provost for Research, Faculty & International Affairs



August 3, 2015

Via Electronic Filing

Regulatory Policy Division
Bureau of Industry and Security
Room 2009B
U.S. Department of Commerce
Washington, DC 20230

RE: RIN 0694-AG32 - Comments on Department of Commerce's Revisions to Definitions in Export Administration Regulations

I. Introduction

The Satellite Industry Association (“SIA”)¹ hereby submits comments on the revisions to definitions in the Export Administration Regulations (“EAR”) proposed by the Department of Commerce’s Bureau of Industry and Security (“BIS”).² SIA appreciates the work BIS has done to implement export control reform and reduce the complexity of the regulations, and the proposed revisions achieve this goal in many ways. SIA has identified some definitions that would benefit from additional clarification or modification to better achieve BIS’ goal. Below is a summary of SIA’s recommendations.

¹ SIA is a U.S.-based trade association providing worldwide representation of the leading satellite operators, service providers, manufacturers, launch services providers, and ground equipment suppliers. Since its creation twenty years ago, SIA has advocated for the unified voice of the U.S. satellite industry on policy, regulatory, and legislative issues affecting the satellite business. For more information, visit www.sia.org. SIA Executive Members include: The Boeing Company; The DIRECTV Group; EchoStar Corporation; Intelsat S.A.; Iridium Communications Inc.; Kratos Defense & Security Solutions; LightSquared; Lockheed Martin Corporation; Northrop Grumman Corporation; SES Americom, Inc.; SSL; and ViaSat, Inc. SIA Associate Members include: ABS US Corp.; Airbus DS SatCom Government, Inc.; Artel, LLC; Cisco; Comtech EF Data Corp.; DRS Technologies, Inc.; Eutelsat America Corp.; Glowlink Communications Technology, Inc.; Harris CapRock Communications; Hughes; iDirect Government Technologies; Inmarsat, Inc.; Kymeta Corporation; Marshall Communications Corporation; MTN Government; O3b Limited; Orbital ATK; Panasonic Avionics Corporation; Row 44, Inc.; TeleCommunication Systems, Inc.; Telesat Canada; TrustComm, Inc.; Ultisat, Inc.; Vencore Inc.; OneWeb; and XTAR, LLC.

² Revision to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31505 (2015) (proposed Jun. 3, 2015) (“Harmonization Rulemaking”).

II. Request for Clarification or Modification

A. Section 734.13 – Definition of “Export”

1. *Section 734.13(a)(1) and (2)*

BIS proposes to remove paragraph (b) of current section 734.2 and create section 734.13(a)(1) and (2) to consolidate the definitions of “export” and “export of technology and software”.³ The revisions appear to remove the “release of technology or software subject to the EAR in a foreign country”⁴ and, as a result, the definition of an export no longer includes disclosing (including oral or visual disclosure) or transferring technology to a foreign person abroad. SIA requests clarification on whether oral or visual disclosures of technology or source code are no longer considered exports or whether they are captured in new section 734.13(a)(1) as a “transmission out of the United States”.⁵

B. Proposed Sections 734.13(a)(3) and 734.14(a)(3) Require Clarification

Under proposed sections 734.13(a)(3) and 734.14(a)(3), an export or reexport occurs when a person transfers

registration, control, or ownership of ... [a] spacecraft subject to the EAR that is not eligible for reexport under License Exception STA (i.e., spacecraft that provide space-based logistics, assembly or servicing of any spacecraft) to a person in or a national of any other country.⁶

This definition appears to carve out all satellites eligible for license exception STA from the definition of an export or reexport. If applied as written, a U.S. satellite manufacturer or operator could transfer control of a commercial communications satellite either in-orbit or on the ground in the U.S. to any country other than those included in Country Group D:5, and the transfer would not qualify as an export because commercial communications satellites are eligible for license exception STA. SIA requests confirmation that BIS intended this result.

C. Section 734.13(b) Criteria for Establishing Most Recent Country of Permanent Residency

SIA requests guidance from BIS on how to establish an individual’s most recent country of permanent residency. SIA understands that few countries offer “permanent residency” akin to a U.S. green card; therefore, guidance on the types of documents that establish an adequate level of residency would be appreciated.

³ *Id.* at 31507.

⁴ 15 CFR 734.2(b)(2)(i).

⁵ *Harmonization Rulemaking*, 80 Fed. Reg. at 31516.

⁶ *Id.*

D. Section 734.14 – Definition of Reexport

Section 734.14 states that a reexport means “an actual shipment or transmission of an item from one foreign country to another foreign country...”. As a general request, does this mean that the shipment of a U.S. origin item from a foreign country back to the U.S. does not constitute a reexport?

E. Section 734.15(a)(3) – “Release”

SIA requests BIS to revise proposed section 734.15(a)(3). The new paragraph defines “release” to include

The application by U.S. persons of “technology” or “software” to situations abroad using personal knowledge or technical experience acquired in the United States, to the extent that the application reveals to a foreign national “technology” or “source code” subject to the EAR.⁷

The relevance of “personal knowledge” or “technical experience” to establishing a “release” is unclear. The essence of proposed paragraph (a)(3) is to capture activities that reveal technology or source code. Rather than introduce vague concepts into the definition, SIA recommends revising the paragraph as follows: “The application by U.S. persons of ‘technology’ or ‘software’ to situations abroad that reveals to a foreign national ‘technology’ or ‘source code’.”

F. Sending or Taking Technology Overseas for Use by a U.S. Person

Proposed section 734.18(a)(4) states that “sending, taking or storing technology or software” is not an export, reexport or retransfer provided that certain conditions are met, one of which is that the data are secured using cryptographic modules.⁸ Proposed section 740.9(a)(3) in turn implies that technology sent in compliance with the requirements of section 740.9 is still an export even if the technology is encrypted.⁹ SIA requests clarification as to whether a U.S. person sending or taking technology overseas on an encrypted device for his personal use or use by another U.S. person is engaged in an export.

Secondarily, SIA requests clarification as to whether the release of technology or software to a U.S. person in a foreign country is an export. The definitions of “export” under section 734.13 and of “release” under section 734.15 only address exports and transfers of technology to foreign persons.

⁷ *Id.*

⁸ *Id.* at 31517.

⁹ *Id.* at 31518.

G. Section 734.18(a)(4)(iv) – Storing Encrypted Technology

In addition to the concerns raised above with new section 734.18(a)(4) is the requirement that the technology is “[n]ot stored in a country listed in Country Group D:5.”¹⁰ SIA requests clarification as to the definition of “not stored in”. Specifically, is the term meant to cover data that are stored on a network located in a country proscribed in ITAR 126.1 or the Russian Federation? Can a U.S. person still send or take technology that is secured using cryptographic modules to the designated countries if the data are to be used by a U.S. person?

H. Section 772.1 – Definitions

1. *“Required” and “Peculiarly Responsible”*

BIS has proposed new definitions for “required” and “peculiarly responsible”.¹¹ SIA notes that the definitions inject additional uncertainty into determining how technology or software may be controlled. Furthermore, the example provided in the definition of “required” does not clarify the definition. The example states:

If production technologies “A”, “B”, and “C” allow production at no more than 399 MHz, then technologies “A”, “B”, and “C” are not “required” to produce the controlled product “X”. If technologies “A”, “B”, “C”, “D” and “E” are used together, a manufacturer can produce product “X” that operates at or above 400 MHz. In this example, technologies “D” and “E” are “required” to make the controlled product and are themselves controlled under the General Technology Note.¹²

In this example, would technology “D” be controlled if technology “E” were not used?

SIA recommends BIS apply the dictionary definition of “required,” which includes “needed” or “essential”, and remove the example.¹³ The dictionary definition will be easier for exporters to implement and therefore is a more effective control.

2. *“Technology”*

The definition of “technology” provided in proposed section 772.1 carves out “[n]on-proprietary general system descriptions”.¹⁴ This carve out implies that general system descriptions that are treated as proprietary are now to be treated as technology controlled under the EAR. This represents a significant expansion in the type of information that qualifies as technology and would increase the regulatory burden on companies in direct contravention to the stated purpose of export control reform. SIA requests that the definition be revised to clarify that

¹⁰ *Harmonization Rulemaking*, 80 Fed. Reg. at 31517.

¹¹ *Id.* at 31519-20.

¹² *Id.*

¹³ TheFreeDictionary.com, available at <http://www.thefreedictionary.com/required>.

¹⁴ *Harmonization Rulemaking*, 80 Fed. Reg. at 31520.

general system descriptions do not qualify as technology whether or not they are treated as proprietary.

* * *

SIA appreciates the opportunity to comment on BIS' proposed revisions to the EAR definitions and contribute to BIS' efforts to harmonize and simplify the export control regulations.

Respectfully submitted,

/s/

SATELLITE INDUSTRY ASSOCIATION

Tom Stroup
President
1200 18th Street NW, Suite 1001
Washington, D.C. 20036
(202) 503-1560

Office of the Vice President for Research and Economic Development

Ms. Hillary Hess, Director
Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security (BIS)
U.S. Department of Commerce (DOC), Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

Submitted Electronically

RE: EAR Amendment – Revisions to Definitions (RIN 0694-AG32 and 15 CFR Part 734)

Dated: August 3, 2015

Dear Ms. Hess:

The University of Alabama at Birmingham (UAB) joins and incorporates by reference, the official positions expressed by the Council of Governmental Relations (COGR), the Association of American Universities (AAU), and the Association of University Export Control Officers (AUECO). In addition to our associated positions, UAB takes this opportunity to comment on the proposed amendment as it specifically relates to our mission-critical sponsored research.

UAB appreciates the joint efforts of the Department of State's Directorate of Defense Trade Controls (DDTC) and the Department of Commerce's Bureau of Industry and Security (BIS) to make export regulations more consistent. We believe that the proposed rules were drafted in good faith to harmonize definitions in ITAR and EAR, with the intent to "facilitate enhanced export compliance and reduce regulatory burdens." Unfortunately, if implemented as proposed, UAB is certain to experience substantial direct academic, research, and financial losses. These unintended consequences would hinder our ability to conduct fundamental research in a teaching and learning environment designed to promote the free exchange of resulting ideas. We discuss below those specific proposals that would impact our organization.

- **Definition of Fundamental Research:** Current §734.8(b) *University based research*, states the criteria to be used by UAB and other accredited U. S. Universities to determine whether research qualifies as *fundamental research*. UAB recommends that this criteria and underlying definition of *fundamental research* be retained in EAR, because it provides a reasonable framework for evaluating proposed research activities, provided all criteria outlined in §734.8(b) are met. Alternatively, we agree with AUECO's suggestion that BIS develop a decision tree tool for determining fundamental research for U.S. Universities that incorporate the current criteria for university based fundamental research.
- **Technology and Software:** Currently §734.3(b) (3) specifically exempts Publicly available technology and software, except software classified under ECCN 5D002 on the Commerce Control List, that: (a) are already published or will be published ;(b) arise during, or result from, fundamental research; (c) are educational in nature; and (d) are included in certain patent applications, as described in § 734.10.

UAB recommends that research involving technology and software as described above, continue to be exempt from the EAR. The proposed changes would inconsistently classify

720E Administration Building
701 20th Street South
205.934.1294
Fax 205.996.6211

marchase@uab.edu
www.uab.edu/research
Mailing Address:
AB 720E
1720 2ND AVE S
BIRMINGHAM AL 35294-0107

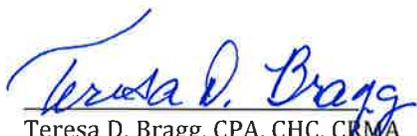
natural-language documents written by a researcher as *technology*, which could be freely shared as arising from fundamental research. Conversely, a related *computer-language* document (i.e., a program in source code), written by the same researcher for the same underlying purpose as the natural language document, would be subject to deemed export restrictions. Such restrictions would require UAB to obtain an increased number of export licenses, while receiving no additional funding to support licensing activities.

- **Supplement No. 1 to Part 734 – Questions and Answers – Technology and Software Subject to the EAR:** UAB recommends that this supplement be retained by the BIS because it serves to clarify and interpret the details changes made in the EAR, which may otherwise be difficult to implement.
- **End to End Encryption Standard §734.18, Activities that are Not Exports, Reexports, or Transfers:** UAB agrees with the proposed standard of the Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) in accordance with NIST guidance or “similarly effective cryptographic means.” This proposed addition is beneficial in that Universities flexibility to use various cryptographic technologies, even while traveling abroad, as long as they sufficiently secure the encrypted technology and software.

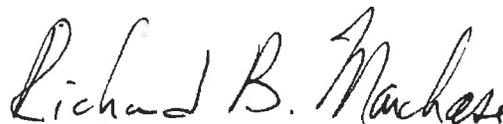
Effective Date of the Final Rule: The regulatory changes, as proposed, would require extensive modifications to our review, negotiation, and assurance functions related to sponsored research agreements. If adopted as proposed, UAB would be required to substantially expand export access controls and obtain export licenses for every foreign national working on any project where the sponsor requests a review prior to publication involving defense related research. UAB would require additional financial resources to continue providing effective export compliance program administration. Based on this potential for increased regulatory burden, we recommend that the effective date be delayed by at least six months.

UAB appreciates this opportunity to provide comments, specific to our organization, on the proposed regulatory changes.

Sincerely,



Teresa D. Bragg, CPA, CHC, CRMA
Empowered Official - Export Control
University Compliance Officer



Richard B. Marchese, PhD
Vice President for Research
and Economic Development



Tom Jackson, PhD
Facility Security Officer



Export Controls Office
University of Cincinnati
P.O. Box 210567
Cincinnati, OH 45221

51 Goodman Drive
Phone: 513-556-1426
Fax: 513-558-2296

August 3, 2015

Ms. Hillary Hess
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230

RE: RIN 0694-AG32

Dear Ms. Hess,

I appreciate the opportunity to respond on behalf of the University of Cincinnati to the proposed Revisions to Definitions in the Export Administration Regulations (EAR) and corresponding changes to the International Traffic in Arms Regulations (ITAR). If the definitions are adopted as proposed, they will have significant impact on U.S. academic institutions. We fully support the Export Control Reform Initiative and submit these comments to request further clarification of the definitions to ensure that U.S. research is safeguarded.

Educational Information

Currently, §734.9 defines “educational information” as information released by instruction in catalog courses and associated teaching laboratories of academic institutions, and §734.3(b)(3)(iii) excludes such information from the scope of the EAR. In the proposed rule, the definition of “educational information” is removed, and §734.3(b)(3)(iii) excludes information and “software” that concern general scientific, mathematical, or engineering principles commonly taught in schools and released by instruction in a catalog course or associated teaching laboratory of an academic institution. The applicability of the exclusion is potentially narrowed by the proposed changes. The concern is that academic institutions will need to consider if other institutions are providing similar curricular to be considered “commonly taught” when developing new curricular. In addition, certain activities that are currently treated as “educational information” may become export controlled if they include more than general principles. A potential issue is raised with the definition of associated teaching laboratory and if that would include such activities as capstone experiences and educational design laboratories. The University environment is open and collaborative with no discrimination on the basis of nationality or citizenship. Academic programs only limit participation by required prerequisites.



The proposed §734.3(b)(3)(iii) could potentially inhibit the ability of U.S. universities to develop new courses in emerging areas of science and engineering. The limitation of the advancement in academic programs would greatly cripple the career options of graduates and the innovation of our country, which would cause a reduction in competitiveness and economic growth. We recommend that the current statement “is released by instruction in catalog courses and associated teaching laboratories of academic institutions” is retained or to include more detail in the description to cover the educational information that the proposed rule removed.

Fundamental Research

The proposed definition of “fundamental research” using the language of NSDD-189 in the EAR and the ITAR is consistent with our understanding. The proposed rule adopts a definition of “applied research” taken from the DFARS (48 CFR part 31.205-18) with an alternate definition adopting OMB Circular A-11 language. The OMB Circular A-11 language reads: “applied research is defined as systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met”. We appreciate the addition of this definition as it is widely understood and suggest that if the DFARS definition of “applied research” is used, that it would be include the rest of 48 CFR part 31.205-18, “Applied research does not include efforts whose principal aim is design, development, or test of specific items or services to be considered for sale; these efforts are within the definition of the term development, defined in this subsection.” The specific statement of “for sale” helps to clearly distinguish between “applied research” and “development” activities.

BIS has also proposed an alternate definition: “fundamental research” means non-proprietary research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community. Clarification of what is considered “non-proprietary” would greatly assist the interpretation of the definition along with prepublication review under specific circumstances.

The proposed definition may be applicable to all organizations and locations, this creates uncertainty in the interpretation of the regulations with the removal of research that is conducted at institutions of higher learning in the U.S., currently §734.8(b). If at all possible, we suggest that the current language of §734.8(b) remain in the EAR as we utilize this definition when making determinations that a research project meets all the criteria to be considered “fundamental research”. If the current language will not be retained, then please outline what would be considered fundamental research at an institution of higher learning within the U.S. and abroad.

“Fundamental research”, “technology”, and “software”

Under the proposed §734.8(a), “technology” that arises during, or results from, fundamental research and is ‘intended to be published’ would not be subject to the EAR. This is a change from the current §734.3(b)(3), under which “publicly available technology and software...[that] arise during, or result from, fundamental research” are not subject to the EAR. We suggest that you revise the proposed definition to include “software” as the proposed rule potentially restricts university research. The concern is that the same “technology” created by a researcher

under fundamental research could be shared freely in a written document but then subject to the regulations if written in source code in a software program. "Software" resulting from university research is "published" as well as "technology", as recognized in the current §734.7(b). The current export definitions in §734.2(b) recognize the similarities between software and technology.

Questions and Answers- Technology and Software Subject to the EAR

We currently utilize the questions and answers found in Supplement No. 1 to part 734 as they assist in confirming interpretations and understanding of the regulations. As they are illustrative to comparable scenarios commonly found in a university setting. The questions and answers are vital to the clarification of the changes and proper interpretation of the regulations.

End to End Encryption Standard

We are most grateful for the exclusion of sending, taking or storing software that is secured using end to end encryption from export activities. The listed activities defined in the addition of §734.18 to the regulations is quite helpful and reduces the regulatory burden of our faculty and staff.

Effective Date of the Final Rule

We recommend a minimum a six month delay in the effective date and that the revised regulations are to be applied to new projects after the effective date. The reason we recommend this timeframe is that the proposed definitions as they are currently written greatly impact our activities. Under the current regulations, we allow time-limited prepublication reviews by sponsors to ensure that proprietary information or patent seeking protection is safeguarded. If the proposed changes to ITAR §120.49(b) are not altered, the final rule will cause significant changes to our business practices and require the development and implementation of new procedures for review and negotiation of sponsored research projects. In addition to new procedures, these changes will require the implementation and monitor of technology control plans and license submissions for the participation of foreign nationals in the research while the prepublication review occurs. Additional training to the affected departments will be conducted and an increase in workload for the current projects to apply the changes retrospectively will require additional staffing for export compliance.

Thank you for considering our comments to these proposed changes.

Sincerely,

Tara L. Wood
Director, Export Controls
University of Cincinnati
Email: tara.wood@uc.edu

July 27, 2015

Regulatory Policy Division
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, DC 20230

Via email to publiccomments@bis.doc.gov

RE: RIN 0694-AG32

Dear Sir or Madam:

The University of Maryland Baltimore, one of twelve institutions of the University System of Maryland, is providing comments in response to the proposed rule on *Revisions to Definitions in the Export Administration Regulations*, RIN 0694-AG32.

BIS specifically solicits comment on “whether the revisions proposed in this rulemaking create gaps, overlaps, or contradictions between the EAR and the ITAR.” We wish to comment on one specific instance of concern: that of prepublication review as related to fundamental research.

EAR 734.8(b)(2) provides that research subject to prepublication review is still “intended to be published” when such review is solely to insure that the publication would not inadvertently divulge proprietary information furnished by the sponsor to the researchers. ITAR 120.49(b) states that researchers must be free to publish “...without any restriction or delay, including U.S. government-imposed access and dissemination controls or research sponsor proprietary information review.”

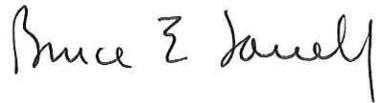
When universities work with industry partners, the research agreement routinely provides for prepublication review to prevent unintended disclosure of a sponsor’s proprietary information. If the ITAR language stands, our industry sponsors will continue to expect the opportunity for prepublication proprietary information review. As such the university would be in a position of turning down or restricting access to research that would, except for the proprietary information review, be considered fundamental research.

We strongly urge that the ITAR language at 120.49(b) be modified to align with the proposed rule at EAR 734.8(b).

BIS solicits comment on “whether the questions and answers in existing Supplement No. 1 to part 734 proposed to be removed by this rulemaking have criteria that should be retained in part 734”. The University of Maryland Baltimore has found the questions and answers very helpful. We would prefer that these be retained within the regulations rather than placed separately on a website. We have used these illustrative and interpretive materials in support of determinations and believe that, if removed and simply posted to a website, they will not have the same influence for decision-making.

We appreciate the export reform efforts undertaken by the Bureau of Industry and Security, and hope that these comments will be helpful in the harmonization process.

Sincerely yours,

A handwritten signature in cursive script that reads "Bruce E. Jarrell".

Bruce Jarrell, MD, FACS
Chief Academic and Research Officer
Senior Vice President

United Technologies Corporation
1101 Pennsylvania Avenue, N.W.
10th Floor
Washington, D.C. 20004-2545



Submitted Via Email

August 3, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry and Security
Room 2099B
U.S. Department of Commerce
Washington, D.C. 20230

Attn: RIN 0694-AG32

Re: Proposed Rule; Comments on Revisions to Definitions in the Export Administration Regulations (80 Fed. Reg. 31505, June 3, 2015)

Dear Ms. Hess:

United Technologies Corporation (“UTC”)¹ appreciates the opportunity to submit these comments to the Bureau of Industry and Security (“BIS”) on the proposed amendments to the Export Administration Regulations (“EAR”) regarding various definitions in order to clarify the scope of activities and information that are covered within these definitions and to harmonize the definitions with the International Traffic in Arms Regulations (“ITAR”). Most significantly, this proposed rule introduces new sections that would exclude from the definitions of export, reexport and transfer (in-country) the electronic transmission and storage of unclassified technical data abroad provided the technical data is sufficiently secured to prevent unauthorized access by foreign persons. The Directorate of Defense Trade Controls (“DDTC”) concurrently published proposed amendments to the ITAR to align and harmonize these definitions, including largely parallel treatment concerning the electronic transmission and storage of technology abroad.

UTC supports the objectives of the BIS and DDTC proposed rulemakings to clarify, harmonize and update, wherever possible, common or similar terms and definitions to facilitate enhanced compliance, promote consistency, and reduce regulatory burdens. In particular, we believe the agencies’ proposals to address the electronic transmission and storage of technical data are critically important to achieving these objectives. The business and information technology (“IT”) environment in which global companies operate has changed profoundly over

¹ UTC is a global, diversified corporation based in Hartford, Connecticut, supplying high technology products and services to the aerospace and building systems industries. UTC’s companies are industry leaders, among them Pratt & Whitney, Sikorsky, UTC Aerospace Systems, UTC Building & Industrial Systems, and United Technologies Research Center.

the past two decades. Increased use of electronic modes of collaboration and communication – such as email, web-based portals, networked shared drives, cloud computing, globally connected enterprise resource planning, engineering and manufacturing systems, etc. – has enhanced greatly the ease and frequency of information sharing. In this environment, the physical (geographic) location of information is less relevant than the security conditions governing access to the information. We strongly encourage and support changes to the regulations that recognize these new global business paradigms and evolve relevant EAR and ITAR definitions, policies, and practices to ensure an effective, harmonized export control regulatory system for the 21st century.

A. § 734.18 Activities that are not exports, reexports or transfers – transmission and storage of technical data and software

UTC supports the addition of EAR § 734.18 describing activities that are not exports, reexports or retransfers and, therefore, do not require authorization from BIS. We commend DDTC and BIS for their proposals to address through regulatory changes some of the longstanding and challenging issues facing industry with regard to compliance with export controls when transmitting, storing and managing technical data (and software) in electronic environments. We fully agree with the principle that in an electronic environment, the standards for defining an export, reexport or retransfer, i.e., a controlled event, should focus on the conditions of *access* to the controlled data and software and not just the physical (geographic) location of the digital bits as they move (in motion) or are stored (at rest). The proposed carve-out in paragraph (a)(4) for sending, taking or storing technical data and software that is secured using cryptographic means is a positive step forward.

Encryption is one instrument in UTC's toolset of security measures to secure and prevent unauthorized access to sensitive and proprietary information, including export-controlled data. UTC primarily uses encryption-based tools in high-risk areas such as securing portable media (e.g., laptops, phones, external storage devices, etc.) and certain transmissions within or outside the company network (e.g., Virtual Private Network ("VPN"), Managed File Transfer, etc.). Encryption is applied through security tools in different ways to achieve data protection, whether the underlying data files are encrypted, or the "pathway" for transmitting data or the electronic "container" for storing data is encrypted. In addition, UTC's IT security program employs various other robust data protection measures based on the nature of the IT system or application, technical and performance requirements, and cost of deployment. The tools include logical access controls such as single or multi-factor authentication, password protection with password length and complexity protocols, and other access restrictions. Logical access controls (as opposed to encryption) are heavily used in IT environments in which data is at rest, such as servers, databases, enterprise IT applications.

1. Clarify the Definition of End-to-End Encryption

Paragraph (a)(4)(ii) requires that technical data or software is secured using end-to-end encryption, which is defined in paragraph (b) as "the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient..." The definition goes on to state that "it involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient..." Such uninterrupted protection can be achieved by

encrypting the underlying data files (i.e., the data is not in clear text and is unreadable without the key) or encrypting the transmission pathway or storage device (i.e., the pathway or device is encrypted, and data moving through the pathway or stored on the device cannot be accessed without the decryption key). It is not clear if the proposed definition requires encryption of the data content or permits encryption protection of the pathway or container.

UTC submits that requiring the data itself be encrypted is an overly narrow application of the concept, and is not a widespread practice for securing data at rest (stored) in IT systems. UTC recommends that BIS revise § 734.18(b) to read as follows:

(b) *Definitions.* For purposes of this section, ‘end-to-end encryption’ means the provision of uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It requires that the originating party encrypt the data or otherwise prevent access to the data through cryptographic means to keep that data secured until received by the intended recipient, where the means to access the data in readable form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider.

The following examples illustrate uses of encryption to secure the pathway or storage media. UTC requires all laptop computers maintain Full Disk Encryption of the hard drive. The entire hard drive is encrypted, so all data and software stored on the hard drive is protected end-to-end although the data files themselves are not encrypted. The employee to whom the laptop is assigned can unencrypt the device by logging into the laptop using their unique network ID and password. Similarly, U.S. person employees on international travel may use a secure VPN connection (i.e., an encrypted tunnel) to access data stored on servers in the United States. Another scenario involves backing up data from a server onto some form of portable electronic media and storing the physical back-up media offsite for disaster recovery purposes. The storage media is encrypted before it is provided to an offsite storage vendor, and remains encrypted at every point during storage unless and until the originator needs to recover the information. We encourage DDTC to clarify the proposed end-to-end encryption standard to encompass cryptographically securing the channel for transmission or the storage medium.

2. Allow Cryptographic Means that are Similarly Effective to FIPS 140-2

The proposed carve-out for transmitting or storing technical data using end-to-end encryption requires that the cryptographic modules be compliant with the National Institute for Standards and Technology (“NIST”) Federal Information Processing Standard Publication 140-2 (“FIPS 140-2”) or be secured using other “similarly effective cryptographic means.” As BIS recognized, although FIPS 140-2 is a widely recognized cryptographic standard used in Federal Government procurement in the United States and for other uses abroad, companies may use hardware and software products that may not be certified to FIPS 140-2 but achieve equivalent encryption-based information security.

As noted above, UTC uses a broad tool set with a variety of solutions to ensure information security for sensitive enterprise data during transmission and at rest. UTC believes

it is important to allow companies the flexibility to use alternate encryption solutions (software and hardware modules) across their IT environment that may not be certified to FIPS 140-2 but provide comparable effectiveness.² It would be the responsibility of the exporter to determine equivalent effectiveness. We urge BIS to maintain the proposed language allowing for use of “similarly effective cryptographic means” to secure data and software in transit or at rest, and have recommended that DDTC adopt the same approach in its final rule.

In addition, we understand that an encryption product may lose its certification in certain circumstances, such as when a security flaw is detected. Such flaws are normally patched rapidly, but the product may have to go through a re-certification process. A cryptographic product that is deployed and in use should not be considered ineligible under the carve-out if it temporarily loses FIPS certification but is recertified within a certain period of time (i.e., one year). Likewise, if a product needs to be re-certified to meet a revision of the standard, it should continue to remain eligible.

3. Other Challenges Involving the Transmission, Storage and Management of Technical Data in IT Environments

In explaining the proposed exclusion for certain encrypted data, BIS cites two examples where controlled technical data may be electronically routed through or stored on foreign servers unbeknownst to the original sender. Specifically, the case of email that might transit a foreign country’s Internet service infrastructure in route to its intended and authorized destination, and the use of mass data storage (cloud storage) where the controlled data may be stored on servers physically located in a foreign country(ies). There are many other examples involving the electronic movement, storage and access to technical data, driven by the business imperatives for international collaboration across a global IT infrastructure. Although the proposed exclusion of certain encrypted data and software from the definitions of export, reexport and retransfer may not directly address these examples, we encourage DDTC and BIS to consider these scenarios as they develop a final rule and in their ongoing review and update of controls as part of the Administration’s Export Control Reform initiative.

- IT datacenter provider hosts servers containing ITAR or EAR data outside the United States. Datacenter employees have physical access to the servers abroad, but cannot access the data stored on the servers due to logical access controls. Database maintenance and other functions requiring access to the data are performed remotely by U.S. persons.
- IT system application hosted on a server in the United States and utilized by non-U.S. subsidiaries. UTC business unit uses an enterprise manufacturing execution system (“MES”) to document, control and manage the manufacturing process and work-in-

² We understand that FIPS 140-2 establishes a Cryptographic Module Validation Program (CMVP), where third-party accredited laboratories perform validation testing of cryptographic modules (both hardware and software). We also understand NIST maintains validation lists of modules/implementations that receive validation certificates. If the requirement for FIPS 140-2 conformity is retained, we urge DDTC to provide explicit guidance on use of the validation lists to confirm that specific encryption products are certified.

process on the factory floor. The MES application is hosted on a server located in the U.S. Non-U.S. subsidiaries of the business unit engaged in the aftermarket maintenance, repair and overhaul of the company's products use the MES system to create, maintain and execute certain repair processes constituting non-U.S. technical data. The data is created and managed wholly outside the U.S., and personnel at the non-U.S. subsidiary only have access to their repair plans in the MES system. Likewise, business unit personnel in the United States cannot access the data (the MES application employs user-level security controls). In this scenario, non-U.S.-origin data, which is not accessed or in any way manipulated in the U.S., should not fall under jurisdiction of the U.S. export control regulations solely because the servers are physically located in the U.S.

B. § 734.3(b), Note to (b)(3) Items subject to the EAR

In a final rule published in June 2014, BIS added a sentence to the definition of "technology" to clarify that "technology" also includes specific information necessary for operation, installation, maintenance, repair, overhaul, refurbishing, or other terms specific in Export Control Classification Numbers ("ECCNs") on the Commerce Control List ("CCL") that control "technology."³ BIS also added Note 2, which stated that "technology" not elsewhere specified on the CCL is designated as EAR99. The preamble stated that note did not change the definition but, together with the new sentence, was intended to provide "additional guidance on the application of the definition based on current BIS practice and past interpretive guidance BIS has provided[.]" BIS now proposes to add a Note to EAR § 734.3(b)(3) to make explicit that information that does not meet the definition of "technology" is not subject to the EAR. UTC appreciates this clear statement regarding BIS' change in practice and brings to your attention two situations that are impacted by this shift.

First, in a final rule published in August 2014, BIS added ECCN 0A998 to control specific oil and gas exploration items, including data.⁴ This entry is specifically intended to control information that does not meet the definition of "technology." In the preamble to this rule, as well as in Q18 of BIS' Frequently Asked Questions for the Russia Sanctions, BIS states that this data is a "commodity." However, with this new note, companies with data classified as ECCN 0A998 would likely determine that their data would not meet the definition of "technology" and conclude that such data is not subject to the EAR. It would be inconsistent to determine otherwise in the clear face of the new language.

Second, UTC notes that the Office of Foreign Assets Control's definition of "informational materials" largely relies upon whether an item is subject to the EAR. This new note potentially creates a situation where information that is of a technical nature but not "technology" and not publicly available would be considered "informational materials" and, therefore, eligible for export to a sanctioned country without a license.

³ Corrections and Clarifications to the Export Administration Regulations; Conforming Changes to the EAR Based on Amendments to the International Traffic in Arms Regulations. 79 Fed. Reg. 62612 (June 5, 2014). The sentence added by the June 4 rule is currently designated as Note 1 to the definition of "Technology."

⁴ Russian Oil Industry Sanctions and Addition of Person to the Entity List. 79 Fed. Reg. 45675 (Aug 6, 2014).

C. § 734.20 Definition of Permanent and Regular Employee

On October 31, 2013, BIS published updated guidance on its website regarding deemed reexports of technology in order to harmonize with certain ITAR definitions as part of Export Control Reform.⁵ In Section V.D of this guidance, BIS referenced DDTC's definition of "regular employee" in ITAR § 120.39 and defined the phrase "permanent and regular employee" for purposes of the EAR. UTC notes that BIS has now included a definition for "permanent and regular employee" in EAR § 734.20(d)(2). We also note use of this term in EAR §750.7(a), as well as a slightly different construction - "*bona fide* regular and permanent employee" - in EAR §§734.20(b)(2) and (c)(2). UTC recommends consistent use of the defined term and also that the term be changed to "regular employee" in all instances because it: (1) maximizes harmonization with the ITAR; and (2) is more accurate because individuals hired by a staffing agency are included and such contract labor are not permanent.

DDTC published a proposed rule in May 2015, which modified its definition of "regular employee" by clarifying that the phrase "long term" indicates that contractual relationship is intended to be one year or longer.⁶ UTC commented that DDTC include the phrase "or other contract employee provider" after each reference to "staffing agency" because it reflects DDTC's current interpretation.⁷ UTC also proposed that DDTC include a Note at the end of the definition to clarify that the contractual relationship can be with the individual, the staffing agency, or other contract employee provider because a company would be more likely to enter into a contract with the staffing agency or contract employee provider, rather than the individual. Consistent with our comments to DDTC and to further harmonize the definitions in the ITAR and EAR, UTC recommends that BIS revise EAR § 734.20(d)(2) to read, as follows:

- (2) "*Regular employee*" means an individual who:
- (a) is permanently and directly employed by the company, or
 - (b) is in a long-term (*i.e.*, 1 year or longer) contractual relationship with the company where the individual:
 - (i) works at the company's facilities or at locations assigned by the company (such as a remote site or on travel);
 - (ii) works under the company's direction and control;
 - (iii) works full time and exclusively for the company;
 - (iv) executes a nondisclosure certification for the company; and
 - (v) where the staffing agency or other contract employee provider that has seconded the individual (if applicable) has no role in the work the individual performs (other than providing that individual for that work) and does not have access to any "technology" other than where specifically authorized by a license or other approval.

⁵ Updated BIS Guidance Regarding the Treatment of Dual and Third Country Nationals with Respect to Deemed Reexports of Technology or Source Code Subject to the EAR (Oct. 31, 2013). *See* <https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-reexport-guidance1>.

⁶ Amendment to the International Traffic in Arms Regulations: Registration and Licensing of U.S. Persons Employed by Foreign Persons, and other Changes. 80 Fed. Reg. 30001 (May 26, 2015).

⁷ Section 3.9 of DDTC's *Guidelines for Preparing Electronic Agreements* states that individuals can be hired through staffing agencies "or other contract employee providers."

Note to paragraph (d)(2): The contractual relationship can be with the individual, the staffing agency or other contract employee provider.

D. §§ 734.13 Export, 734.14 Reexport

UTC understands that the intention of EAR §§ 734.13(a)(6) and 734.14(a)(4) is to make the provision of the means of access (*e.g.*, providing decryption keys, passwords, network access codes, etc.) to encrypted data an “export” or “reexport.” For consistency, UTC recommends that BIS utilize the same word construction from the definition of “technology” in §§ 734.13(a)(6) and 734.14(a)(4). This would also align better with the proposed counterpart provisions in ITAR §§ 120.17(a)(6) and 120.19(a)(4).

BIS has maintained a long-standing position of drawing a distinction between actual access and potential access. UTC understands that BIS intends to retain this distinction, as BIS explains that the “mere act of providing physical access to unsecured “technology” will not, however, be a controlled event...” However, the current proposal defines an export (and reexport) to be the provision of the means of access with “knowledge” that it “will cause or permit” the transfer of controlled technology. UTC believes that this phrasing is confusing and appears to undercut BIS’ existing position. First, it is unusual for BIS to include a knowledge standard outside of catch-all, end-use or end-user controls. Second, the language does not account for whether the recipient has accessed the controlled technology and “permit” may include situations where the foreign national has the ability to access the “technology” but does not.

The distinction between DDTC’s and BIS’ position on access is important and UTC believes it merits sufficient explanation directly in the EAR. Therefore, UTC recommends that BIS revise EAR § 734.13(a)(6) to read, as follows, and that conforming changes be made to § 734.14(a)(4):

(6) Releasing or otherwise transferring information (*e.g.*, decryption keys, network codes, passwords) or “software,” or otherwise providing access to other “technology” in clear text or “software” to a foreign national.

Note to paragraph (6): The mere act of releasing or otherwise transferring the information (*e.g.*, decryption keys, network codes, passwords) or “software,” or otherwise providing means of access, is not a controlled event until the foreign national applies it and accesses the “technology” in clear text or “software.”

In comments submitted in response to DDTC’s companion rule, we encourage DDTC to adopt the BIS formulation to achieve a common, harmonized standard in this area.

E. § 740.9 Temporary imports, exports, reexports and transfers (in-country) (TMP)

1. Remove additional documentation requirement for foreign nationals

UTC acknowledges that existing § 740.9(a)(3)(i)(B) already includes additional recordkeeping requirements that only apply to foreign nationals. This requirement has been carried over into proposed § 740.9(a)(3)(v). UTC does not agree with this requirement because it: (1) creates a different standard for use of the exception for foreign nationals that does not apply to U.S. persons employed by the same employer; (2) is redundant to the requirement set forth in § 740.9(a)(3)(i); and (3) imposes an extra burden on the employer upon each instance of travel to document an underlying premise that has already been established – namely, that the foreign national requires the technology for their activities abroad on behalf of the employer. If there was no need for the foreign national to have the technology, the authorization would not be in place and the requirement in § 740.9(a)(3)(i) would not be satisfied. Therefore, UTC recommends that subparagraph (v) be removed.

UTC also recommends that reexports and transfers (in-country) remain in scope of the exception. Currently, EAR §740.9(a)(3) authorizes use of the exception for “exports, reexports, and transfers (in-country).” However, BIS has narrowed the scope of this exception to exports, which limits the activity to shipments/transmissions out of the United States. This change effectively excludes from its scope that which is permissible today, which will have a negative impact on U.S. person employers. The change would mean that an employee would be limited to export activity and would not be able to transfer the technology to authorized persons or travel onward to third countries with the same technology.

2. Expand scope to include foreign subsidiaries and affiliates of U.S. persons

UTC notes that EAR § 740.9(a)(3)(iii) restricts only U.S. persons to employment by the U.S. government or a U.S. person employer, with no similar restriction on foreign nationals. We believe this is an oversight and the intention is to cover both U.S and foreign national employees. This can be corrected by using the term “individual” to reference the employee in this subparagraph. However, UTC recommends that BIS expand this exemption to include foreign subsidiaries and affiliates of U.S. persons.

If the condition in subparagraph (i) is met – that the foreign national is already authorized to receive the technical data - then the U.S. Government has already determined that such person is “trusted.” Accordingly, if the additional conditions in subparagraph (ii) are met with respect to use and security precautions, the risk of permitting employees of foreign subsidiaries and affiliates of U.S. persons to travel abroad with technology is no different than permitting employees who are working for U.S. affiliates to travel abroad. The U.S. person assumes responsibility as a licensee when its companies engage in activities under the U.S. person’s EAR licenses in accordance with EAR § 750.7(d). Permitting foreign subsidiaries and affiliates of U.S. persons to have a similar authorization as U.S.-based affiliates for employees to travel with EAR technology under prescribed circumstances would greatly benefit global enterprises.

3. Remove requirement to encrypt technical data from security measures

UTC concurs with incorporating affirmative obligations to secure technology. In addition to export compliance considerations, use of security precautions such as firewalls, use of passwords and secure network connections are sound information security practices intended

to prevent unauthorized access to intellectual property, business proprietary information, technology and other types of confidential information. Among the types of security precautions identified in the proposed rule is encrypting the technology. UTC is unclear whether BIS' intention was that they underlying information be separately encrypted while at rest, in addition to securing the "pathway" to access the technology. UTC submits that requiring that the underlying technology also be encrypted is disproportionately burdensome. Further, if the pathway to access the technology is properly secured by use of secure network connections, firewalls, passwords and the like, separately encrypting the technology at rest should not be mandatory.

As written, § 740.9(a)(3)(ii) appears to be a proscriptive list of security techniques, requiring all to be used, which may not be effective, practical, or even necessary, depending on the application. This may not have been BIS' intent, but it is the meaning of the entry. UTC recommends revision to clarify that adequate security measures need to be used but that companies can choose which measures should be implemented.

For the reasons described above, UTC recommends that § 740.9(a)(3) be modified to read as follows:

(a) ***

(3) "Technology," regardless of media or format, exported, reexported, or transferred (in-country) by or to an individual who is travelling or on temporary assignment abroad subject to the following restrictions:

(i) The individual is a "regular employee" of the U.S. government or a U.S. person (including foreign subsidiaries and affiliates of a U.S. person).

(ii) Foreign nationals may only export, reexport or receive such "technology" as they are authorized to receive through a separate license or other approval.

(iii) The "technology" exported or reexported under this exception is to be possessed or used by the employee. Any such "technology" may be retransferred by the employee to a third party, only if there is a separate license or other approval for the third party to receive the "technology."

(iv) Sufficient security precautions are used to prevent unauthorized access to the "technology." Such security precautions may include encryption of the "technology;" the use of secure network connections, such as virtual private networks; the use of passwords or other access restrictions on the electronic device or media on which the "technology" is stored; or the use of firewalls.

(v) "Technology" authorized under this exemption may not be used for foreign production purposes or for defense services unless authorized through a license or other approval.

F. § 772.1 Definition of Peculiarly Responsible and Required

UTC commends BIS for the effort to clarify the interpretation of the term “required,” and to harmonize the interpretation with a proposed new definition in the ITAR. However, we believe that defining “peculiarly responsible” using a “catch and release” format has serious drawbacks, and recommend that the proposed definition be deleted.

In some cases, the proposed definition “peculiarly responsible” will control more than is currently captured under the EAR’s definition of “Required.” The performance levels, characteristics, or functions of “technology” can be controlled higher than the commodities that result from the “technology.” For example, ECCN 9E003.a.5 is “technology” for the “development” and “production” of cooled turbine blades, vanes, and tip shrouds and controlled as National Security 1. Such commodities, when part of a production 9A991.c or .d engine, are themselves 9A991.c, an AT-only control. Per the proposed item (3) release of “peculiarly responsible,” because the 9E003.a.5 “development” and “production” data is used in or with the AT-only commodity, such data cannot be “peculiarly responsible” and, therefore, it cannot be “required” for 9E003.a.5. Further, per the BIS Advisory Opinion of March 25, 2014, the term “required” applies to all ECCNs controlling “technology” regardless of whether the ECCN specifically refers to the GTN or uses the term “required.” As the information to design or produce the turbine components is not “required”, it falls to EAR99. We believe this clearly is not the intent of the proposed definition.

The proposed definition as stated would make the General Technology Note (GTN) an empty box. The GTN controls “technology” “required” for the “development”, “production”, or “use” of a controlled product, even if that “technology” is applicable to a product controlled at a lower level. In order for the GTN to apply, the subject “technology” must be “required.” Per the definition, if that information is used in or with (i.e., applicable to) a production AT-only item (i.e., item of lower control), the information is not “peculiarly responsible” and, therefore, not “required” per the item (3) release. Additionally, releases (4) and (6) would make information not “peculiarly responsible” and, therefore, not “required” simply by documenting contemplated applications of the technology to AT-only commodities, again making the GTN an empty box.

The proposed definition also may result in over-control of certain technologies. Consider information unique to the production of a blade meeting the temperature thresholds in 9E003.a.4, but which is unrelated with the temperature capabilities of the blade. For example, instructions for grinding off excess metal from the fir tree portion of the blade after casting. Under the current definition, such information is necessary for the production of the blade, but contributes nothing towards the ability of the blade to meet or exceed the temperature threshold that triggers control and, therefore, would not be considered 9E003.a.4 technology. Under the proposed definition, since the information is used in production of the controlled blade, it is “caught,” and because it is unique to that particular blade, it would not be released. Under the proposed definition, the information would be considered “peculiarly responsible” and would be controlled under ECCN 9E003.a.4

Further, under the proposed “catch” in the definition, an item is “peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions” if it is

used in or for use in a variety of EAR activities. In this structure, the capability or lack thereof of the item to “achieve or exceed the controlled performance levels...” is replaced by the basic test of the item being “used in or for use in” various EAR activities. The capability threshold is rendered meaningless for purposes of the “catch,” which would result in capturing all of the “mundane” technical data necessary to produce the part, but not “required” under the present definition. This is a significant increase in the scope of “required.” Of course, much of this mundane technology would be “released” in paragraphs (1) through (6), but that would require an extensive analysis of all the technology associated with the item, which would be a significant and unnecessary additional burden over the status quo.

Additionally, the “catch-and-release” format of the proposed definition would overly complicate “specially designed.” The term ‘peculiarly responsible’ appears in the EAR in only two places – the defined term “required” and in the ‘catch’ paragraph (a)(1) of “specially designed” (and subsequent clarifying notes). The effect would be that when analyzing an item against “specially designed”, the ‘catch’ paragraph would require an additional ‘catch and release’ analysis of “peculiarly responsible” before moving on to the ‘release’ of “specially designed.” To further complicate matters, the proposed “peculiarly responsible” has a catch for items (i.e., commodities, software, and technology), releases for items (1), (4), (5), and (6), and the (3) release is reserved for “information.” This will greatly complicate any “specially designed” analysis. If BIS does not intend for the term “peculiarly responsible” in “specially designed” to reflect the defined term, the use of the same term in different ways will cause confusion.

The last drawback is one of style and construction. We believe a defined term (“required”) should not be defined directly by yet another defined term (“peculiarly responsible.”) UTC proposes maintaining the EAR’s existing definition and illustrative example of “required” technology, and eliminating the proposed definition of “peculiarly responsible.”

G. § 772.1 Definition of Proscribed Person

BIS has proposed a new definition for “proscribed person” as “a person who is prohibited from receiving the items at issue or participating in a transaction that is subject to the EAR without authorization by virtue of U.S. law, such as persons on the Entity List, Specially Designated Nationals, or debarred parties.” UTC finds the wording to be overly broad and the illustrative examples to be potentially confusing because they appear to: (a) define a person as a “proscribed person” if they are designated on a list pursuant to *any* U.S. law, some of which may have no export control nexus; and (b) bring activity that might otherwise not be prohibited by the EAR within the scope of the EAR. For example, the Office of Foreign Assets Control is primarily responsible for designating and maintaining lists of Specially Designated Nationals (“SDNs”) under the various sanctions programs it implements. U.S. persons are generally prohibited from engaging in transactions with SDNs, but these prohibitions do not extend to the provision of items subject to the EAR to SDNs by foreign persons absent a specific prohibition in the EAR. UTC notes that BIS has targeted only certain Executive Orders and SDN programs in Part 744 (e.g., §§ 744.8, 744.12, 744.14). If a broader prohibition existed in the EAR to cover all SDNs, those specific provisions would not be necessary.

Although UTC would agree with such an outcome for SDNs, there are lists implemented pursuant to other U.S. laws with no nexus to export control. For example, a person listed in the Excluded Party List System (now managed by the System for Award Management) is “debarred” under U.S. law but such debarment typically pertains to government contracting or prohibits the party from receiving certain government benefits or grants for reasons that have no connection to export control laws. Absent action by BIS to debar the person or identify the person on a list managed by BIS, UTC submits that such a person is not a “proscribed party.” However, this definition may create confusion due to its generic reference to “debarred parties.” UTC recommends that BIS revise the definition of “proscribed person” by deleting the phrase “by virtue of U.S. law” and removing references to SDNs and debarred parties.

BIS has revised EAR § 750.7(a) to specify that a license authorizing release of technology to an entity also authorizes the release of the technology to the entity’s foreign nationals who are permanent and regular employees and who are not “proscribed persons under U.S. law.” As written, this language appears to impose an obligation on the license applicant to ensure that a third party’s foreign nationals are not “proscribed persons.” UTC objects to any requirement that an applicant must directly screen the foreign nationals of an entity that will receive technology under its license. Conducting such screening would require the entity to provide a by name list of such employees, and potentially additional personal information as may be needed for the applicant to verify whether a potential match is in fact a true match to a “proscribed person.” Not only would this be impractical and burdensome for the applicant, it may violate the anti-discrimination, human rights and privacy laws of the countries in which those foreign nationals are resident. If the entity receiving the technology is to conduct the screening directly, EAR § 750.7(a) provides no clear statement to that effect and the entity may also be similarly constrained from conducting such screening pursuant to domestic law.

Complexities raised by this proposed language include whether an applicant is prohibited from providing technology to an entity that refuses to provide the names of its employees for screening by the applicant or refuses to screen them directly, and whether it is adequate for an entity to provide assurances that none of its employees are “proscribed parties” or some general certification regarding EAR compliance. If this change is to become final, BIS needs to provide specific guidance to industry on how this obligation is satisfied.

UTC notes that the phrase “proscribed person under U.S. law” is also used in EAR §§ 734.20(b)(2) and (c)(2). For the reasons already articulated above, UTC believes that this screening requirement will pose significant challenges for foreign persons to implement. Consistent with the changes that UTC recommends above to the definition of “proscribed person,” UTC further recommends that “under U.S. law” be deleted in each instance where BIS uses the phrase “proscribed person under U.S. law” in the EAR.

H. § 772.1 Definition of Technology

Paragraph (a)(1) defines “technology” to include “information gleaned through visual inspection.” UTC recommends replacing the word “gleaned” with “revealed” in order to align with the language used in the proposed definition of “release” in EAR § 734.15(a)(1). The use

of the term “glean” implies the value of the information is based on the capability of the viewer, which is unknowable and unquantifiable. The use of the term “reveal” is a more objective measure of what information is provided by the visual inspection.

In the Note to Paragraph (a)(1), because “development” stops short of serial production, the term “production” must be added, otherwise the instructions for the serial production of Y by modifying existing stocks of X would not constitute technical data under the ITAR. UTC suggests the following revision:

NOTE TO PARAGRAPH (a)(1): The modification of an existing item creates a new item and technical data for the modification is technical data for the development or production of the new item.

Paragraph (b) defines specific types of information that do not constitute “technology,” including in (b)(1) “non-proprietary general system descriptions.” We recommend that the modifier “non-proprietary” be deleted, as the way a company chooses to restrict such information in non-public settings has no bearing on whether the information is technical data or not. General system descriptions may be included in various types of business documents, such as proposals, that are treated as proprietary for commercial reasons. It is understood that the term “general” may cause confusion as to the bounds of “general system descriptions,” but the addition of “non-proprietary” does not provide clarification. Additionally, it should be made clear that the exclusion is not limited to “systems,” as the defined term is used, but also should cover general descriptions of parts, components, accessories, attachments, firmware, software, and end-items.

* * *

For additional information, please contact the undersigned at (202) 336-7467 or peter.jordan@utc.com or Christine Lee at (202) 336-7458 or christine.lee@utc.com.

Sincerely,



Peter Jordan

Director, Senior International Trade Counsel