July 28, 2015

Sent via email to: publiccomments@bis.doc.gov and DDTCPublicComments@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.

<u>Definition of Technology</u>

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.

<u>Definition of "Export"</u>

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."

<u>Definition of Reexport & Deemed Reexport</u>

The comments and recommendations above regarding "export," "deemed export," and "or permit" also apply to "reexport" and "deemed reexport."

<u>Activities That Are Not Exports, Reexports, Releases, Retransfers, or Transfers</u>

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,

Ken Montgomery
Vice President, International Trade Regulation & Compliance