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 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

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 ("CEECR")[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 CEECR 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 ("CEECR") 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(l). 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. <u>"Activities that are not exports reexports, or transfers" Under the EAR and ITAR</u>

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 <u>stored</u> 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 <u>stored</u> 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. <u>"Activities that are not 'deemed reexports'" Under the EAR</u>

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. <u>"Knowledge" and "Violations" Under the June 3 Proposed Rules</u>

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 <u>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</u>.

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 result*s.

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 definition[4] -- 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 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, then 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. <u>"Required" Under the DDTC Proposed Rule</u>

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, "Peculiary 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" (s*ee* 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 testing 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 capabilities[8] **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