August 3, 2015

C. Edward Peartree
Director, Office of Defense Trade Controls Policy
Directorate of Defense Trade Controls
U.S. Department of State
Washington, D.C. 20037

Hillary Hess
Director, Regulatory Policy Division
Office of Exporter Services
Bureau of Industry & Security
U.S. Department of Commerce
Washington, D.C. 20230

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

Dear Mr. Peartree and Ms. Hess,

The Aerospace Industries Association (AIA) and our member companies welcome the opportunity to provide comment in response the Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), (80 Fed. Reg. 31, 525 and 80 Fed. Reg. 31, 505). AIA continues to support the President's Export Control Reform Initiative (ECR) and views the harmonization of definitions across the ITAR and EAR a critical step in the ECR process, encouraging consistency of classification and application.

Comments on Proposed Revisions to Definitions in the ITAR and EAR

§ 120.6 Defense Article.

1. AIA supports the changes to the definition of Defense Article and the removal of software to further align with the EAR. In our review, we recognized a potential oversight to the proposed changes to § 120.6(a). It is understood that * * * means the remaining paragraph language of (a) remains intact, to include the original exclusion language "*It does not include basic marketing information on function or purpose or general system descriptions*." AIA recommends this language be removed from § 120.6(a) as it will be captured in the revised definition of technical data.

§ 120.10 Technical data, § 772 Technology

1. The proposed language at § 120.10(a)(1) includes *installation* in the definition of technical data. In comparing the Note to Paragraph (a)(2) of 120.9, it would appear that the act of installation is one that does not require technical data. If installation does not require technical data, then it would appear to be contradictory to include the term *installation* in the definition of technical

data. AIA recommends the removal of the term *installation* in the definition of technical data. To establish consistency, AIA additionally recommends the removal of the term *installation* in the definition of technology.

2. We recommend the removal of the phrase "…or information gleaned through visual inspection;" from paragraph (a)(1) as it relates to a form or method in which technical data may be transferred, i.e. "exported", rather than what information constitutes technical data.

3. We do not agree with the addition of (a)(5) in the definition of technical data and technology. Decryption keys, network access codes and passwords are not in and of themselves export controlled items. AIA understands the goal with this change is to capture the event of a foreign person accessing encrypted controlled information, and as such AIA recommends that DDTC and BIS consider moving the language in (a)(5) to the definition of Release at and create a new section:

   (a)(3) Accessing encrypted technical data by applying a decryption key, network access code or password.

   Fundamentally, if decryption keys, network access codes and passwords were technical data, sending a decryption key, network access code or password to the wrong non-U.S. person would be considered an export violation, even if possession of the key, code or password was incapable of being used. For example, if Mr. John Smith, a non-U.S. person, received encrypted information, but the key, code or password was sent to different John Smith that was not in the same location or even same company as the recipient of the encrypted information, the wrong John Smith could not use the key, code or password and possession would be meaningless.

   Additional rationale for removing decryption keys, network access codes and passwords from the definition is if an export controlled document is encrypted and emailed, the password could be a simple phrase to open the document (e.g., exporting is fun). This password, by way of this definition, is now export controlled and must be treated appropriately meaning all instances where this phrase appears instantly becomes export controlled. Taking this argument to another level, all derivative usage of the password phrase is also export controlled. Industry is ill-equipped to manage such an overreaching application of controls to passwords.

   Finally, AIA could not readily identify which USML category or ECCN would capture the controls of passwords and decryption keys. Their absence from the USML and CCL supports the argument that the event of accessing the data is what DDTC and BIS are trying to control rather than the passwords and decryption keys themselves.

4. We recommend the removal of the term "non-proprietary" from the term "~~non-proprietary~~ general system descriptions;" as whether data is proprietary does not indicate whether something is technical data or not. Many proposals are proprietary (e.g., for commercial reasons) and contain general system descriptions. Companies make business decisions to describe certain systems descriptions as "proprietary" for various reasons. It would unnecessarily serve as a "chilling effect" on companies if they were aware the mere act of describing a description as proprietary would make it technical data. Further, including this wording is an increase in control. The number of licenses would increase exponentially as a result of controlling propriety data, which would significantly impact license processing times. This would be inconsistent with one of the goals of ECR to limit export control over those

articles or information most important to the national security and foreign policy interests of the United States.

5. We note that DDTC has specifically called out "Telemetry data" in 120.10(b)(3) as not being Technical Data, yet AIA believes this is already established by Note 3 to Paragraph (f) to USML Category XV (Spacecraft). If it is nonetheless the intention of DDTC to specifically identify telemetry data in 120.10(b), then AIA recommends adding a new subparagraph 120.10(b)(4) that would also specifically identify that "activities and technology and other information directly related to or required for the spaceflight passenger or participant experience" as described in Note 2 to paragraph (f) of USML Category XV are also not "technical data."

   That said, there could be other instances driven by notes to USML Categories where data has been or will be specifically excluded from the definition of "technical data" so the more appropriate solution may be to simply remove sub-paragraph (b)(3) to 120.10, or amend its text to state "any technical data or other such information that is specifically identified within the USML, including notes thereto, as not being subject to the ITAR."

§ 120.17 Export, § 734.13 Export

1. AIA requests the removal of (a)(6) from the definitions of Export as our recommendation is to move this requirement to the definition of Release (see above reference) and to amend the proposed § 120.17(a)(1) and § 734.13(a)(1) to

"(a)(1) An actual shipment, *release*, or transmission out of the United States,"

   AIA would like to emphasize its concern with the language utilized in the proposed definition '*providing physical access that would allow access to other technical data'*. This language is quite broad and could be interpreted to mean that physical access to a room where technical data happens to reside and is not intended to be transferred to the foreign person would be considered an export. AIA believes that the measures industry takes to physically control technical data on their premises in order to comply with the ITAR, EAR and NISPOM, as well as company policies on securing company data, are sufficient to ensure that controlled information is not arbitrarily provided to a foreign person. The removal of (a)(6) addresses this concern.

2. The proposed definition of "export" adds paragraph (b) which explicitly states that release of "technical data" to a foreign person is deemed to be an "export" to all countries in which the foreign person has held citizenship or holds permanent residency. As between the ITAR and the EAR there are two standards, namely one that includes, "all previous citizenships" versus only country of last citizenship obtained. Maintaining two different standards increases the regulatory burden on U.S. exporters and is inconsistent with the goal of Export Control Reform to harmonize the two sets of regulations.

   We recommend that the § 120.17 be modified to remove, ". . . and all countries in which the foreign person has held citizenship" to read as follows:

   "Any release in the United States of technical data or software to a foreign person is a deemed export to ~~**all countries in which the foreign person has held citizenship**~~ the foreign person's most recent country of citizenship or permanent residency."

§ 120.19 Reexport, § 734.14 Rexport

AIA requests the removal of (a)(4) from the definitions of Reexport as our recommendation is to move this requirement to the definition of Release (see above reference) and to amend the proposed § 120.19(a)(1) and §734.14(a)(1) respectively to:

"(a)(1) An actual shipment, *release*, or transmission of a defense article…"
"(a)(1) An actual shipment, *release*, or transmission of an item…"

§ 120.46 Required

We recommend including in Note 3 to paragraph (a) the following example for illustrative purposes:

Note 3 to paragraph (a): An illustration of determining whether technical data" is 'peculiarly responsible" for achieving or exceeding controlled performance levels, characteristics, or functions' is as follows: Assume product "X" is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies "A", "B", and "C" allow production at no more than 399 MHz, then technologies "A", "B", and "C" are *not peculiarly responsible* for producing the controlled product "X". However, if technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can produce product "X" that operates at or above 400 MHz. In this example, technologies "D" and "E" *were peculiarly responsible* for making the controlled product and are themselves "required" and therefore controlled as "technical data."

§120.47 Development

The last sentence in this section of the proposed rule states, "*Development includes modification of the design of an existing item.*"

This statement is overly broad and AIA recommends rewriting it as follows: "*Development includes modification of the design of an existing item only when it alters the function or performance capabilities. It does not include modifications of items with equivalent form and fit."* Additionally this aligns with the EAR definition of development.

§ 120.49 Technical data that arises during, or results from, fundamental research.

AIA believes the word 'located' has been extraneously added to the end of § 120.49(a)(1) and suggest it be deleted.

§ 120.52 Activities that are not exports, reexports, or retransfers, § 734.18

1. It was noted in the proposed subparagraph (b) that the term 'given' was utilized rather than 'released'. AIA recommends the following edits: "…. where the means to access the data in unencrypted form is not *released* to any third party ……"

2. Level of security: The rule states, "Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors…" We recommend that the rule specify the modules must be compliant with FIPS 140-2, Level 1. FIPS 140-2 acknowledges four levels of security, and since the data in question is unclassified it should be subject to Level 1.

3. Scope of NIST publications: "Guidance provided in current U.S. National Institute for Standards and Technology publications" could be interpreted to have nearly an unlimited scope due to the large volume of relevant NIST publications. The rule should cite NIST Special Publication SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* as the reference standard for this clause. The controls selected from SP 800-53 should not exceed those in Table 1 of DFARS 252.204-7012, Safeguarding *of Unclassified Controlled Technical Information*.

4. Revision implementation: As written, each time NIST published a revision would cause IT systems to export until they are brought into compliance with the new revision. The rule should allow compliance with the prior NIST revision for one year beyond the publication date.

5. The proposed rule states: "(3) Shipping, moving, or transferring defense articles between or among the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands or any territory, dependency, or possession of the United States as listed in Schedule C, Classification Codes and Descriptions for U.S. Export Statistics, issued by the Bureau of the Census; ***and*** (4) Sending, taking, or storing technical data or software that is…"

   We recommend that the word "and" be changed to "or" to clarify these activities are not conjunctive.

§ 120.9 Defense Services

1. Coordination with 80 FR 30001 (Note 1 to paragraph (a)(1)): The proposed rules in 80 FR 31505 and 80 FR 30001 deal with the same subject and should be published with the same effective date.

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

3. Scope of USML Paragraph (Note 1 to paragraph (a)(1) of proposed 120.9): The language "in the same USML paragraph or accessed" is excessively broad because USML paragraphs are themselves very broad and thus impute to U.S. persons "knowledge" of technical data where

none exists. For example, in Category XI—Military Electronics, paragraph "(a)" includes both "[a]ctive or passive acoustic array sensing systems" and "[r]adar systems and equipment," two largely different disciplines of engineering. As a consequence, potentially many more U.S. persons would fall under this clause than envisioned by DDTC. We recommend instead using "the same USML paragraph subsection."

4. Country of Origin for Programs and Technical Data (Note 1 to paragraph (a)(1) of proposed 120.9): If knowledge is to be imputed, the rule should be particular to U.S. development activity and U.S.-origin technical data. It is unreasonable to control as a defense service under the ITAR the activities of a natural person born in a foreign country and currently working for a foreign employer in that country and only having defense program experience in that country, simply because the natural person acquired U.S. person status.

5. Note to paragraph (a)(1) includes, "…or accessed (physically or electronically) technical data directly related to the defense article that is the subject of the assistance, prior to performing the service."

   We recommend revising or removing this language because (1) the term "access" is too broad as it does not necessarily involve actual access to the technical data, and (2) the language "prior to" does not have any reasonable contemporaneous time reference, meaning it could have been at any past point in a lifetime. As a result, as written, "knowledge of U.S.-origin technical data" could be presumed if, 20 years prior to performing a service, an individual accessed a file containing technical data even though the individual did not study or utilize such data at that time or since.

§ 120.11 Public Domain, § 127.1 Violations

These sections refer in several instances to a general "knowledge" standard. AIA believes that depending on the knowledge standard applied, the text could impose a severe administrative burden on corporate persons. If knowledge is imputed by possession of historical records, persons may be obligated to research historical archives to determine whether or not they had "knowledge" that information made publicly available in the past was unauthorized. The language should be reframed to be forward-looking and apply a strict standard of "knowledge."

§ 125.4(b)(9) Exemptions of general applicability.

1. AIA believes that this language unnecessarily restricts the exemption use for long-term assignments abroad and the utilization of expatriates living in the foreign country. Many defense contractors have contracts servicing U.S. installations abroad that at the end of the negotiated term are renewed; keeping the employee abroad for a longer period of time. AIA could not readily identify the rationale for limiting the exemption to the amount of time the U.S. employee happens to be abroad. When an employee receives technical data while abroad and returns to the U.S. in two weeks, two years, or twenty years, there is no change to the original export. AIA supports the exemption as it is currently applied, and keeping the proposed language in the exemption will hamper the defense industry's ability to support long term contracts for the U.S. military performed in foreign locations; most likely resulting in obtaining export licenses that are currently not required and generating a burden to both the government and industry. Therefore, AIA requests that the language be removed and § 125.4(b)(9) be revised as outlined below:

"*(b)(9) Technical data, including classified information, regardless of media or format, exported by or to a U.S. person or foreign person employee of a U.S. person is subject to the following restrictions…*"

2. The proposed rule paragraph (vi) states, "Classified information is sent or taken outside the United States in accordance with the requirements of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case such guidance must be followed)."

   We request clarification as to whether a party would be at risk of violating the NISPOM if they were to follow the guidance of DDTC.

§ 127.1(b)(4) Violations, § 764.2(l) Violations

AIA requests the removal of § 127.1(b)(4) as our recommendations to amend the proposed definitions of Export at §120.17(a)(1) and Reexport at §120.19(a)(1) would not warrant a change to §127.1 as violations occur when a defense article or technical data is exported or reexported unlawfully as described. We believe § 127.1(a)(1) is sufficient as written and would capture the exposure addressed by the proposed language at § 127.1(b)(4).

Similarly, AIA requests the removal of § 764.2(l) in its entirety as the current language of § 764.2 is adequate.

EAR §§ 734.20 and 750.7 Permanent and Regular Employee

1. AIA's member companies disagree with the proposed definition and use of the phrase "permanent and regular employee" in §§ 734.20 and 750.7(a) to require employment for 1 year or longer. In practice, the term "permanent and regular employee" generally is applied to contract or contingent workers in foreign facilities. Mandating a period of 1 year or longer for the relationship significantly compromises the ability of a non-US defense company to take advantage of the provisions that use this phrase. Many companies do not employ contract workers for periods of a year or longer because doing so can create a risk under labor and employment law that the contract worker would take legal action to acquire the benefits and other rights of employees.

   The five specific criteria enumerated under §734.20(d)(2) are adequate to ensure appropriate control of EAR data in that the worker must: (i) work at the company's facilities; (ii) work under the company's direction and control; (iii) work full time and exclusively for the company; (iv) execute nondisclosure certifications for the company and (v) not be taking direction from the staffing company. Why is it necessary for the relationship to be "long term" if those criteria are satisfied? The company engaging the contract employee will be responsible for the conduct of the worker regardless. The company can decide the length of relationship that would be appropriate given these competing considerations.

   Moreover, the timing requirement does not necessarily apply or make sense in other contexts. What if a company hires an individual for permanent employment and the employee quits after 30 days? There ultimately would be no "long term" relationship under those circumstances

either, yet it is not clear in the proposed definition and use of the phrase whether the employee would fall under the "permanent and regular" definition after being hired.

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

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

§ 734.20 Activities that are not ''deemed reexports.''
(b) Release to A:5 nationals…
(1) * * *5 nationals…
(2) The foreign national is a regular ~~and permanent~~ employee…
(c) Release to other than A:5 nationals…
(1) * * *release to other than A:5 nationals.
(2) The foreign national is a regular ~~and permanent~~ employee…
(d) Definitions
(1) * * *
(2) "~~Permanent and~~ is an individual who:
(a) Is ~~permanently (i.e., for not less than a year) and~~ directly employed by an entity, or
(b) Is a contract employee who:
(i) Is in a ~~long-term~~ contractual relationship with the company…

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

AIA appreciates the opportunity to provide comments and looks forward to continue to work with DDTC and BIS as the U.S. Government addresses additional areas of reform.

Best Regards,

Remy Nathan
Vice President – International Affairs
Aerospace Industries Association