Lockheed Martin Corporation
2121 Crystal Drive Suite 100 Arlington, VA 22202
Telephone 703-413-5600 Facsimile 703-413-5631

LOCKHEED MARTIN

August 3, 2015

Submitted Via E-Mail (DDTCPublicComments@state.gov) & (publiccomments@bis.doc.gov)

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

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

Re: Comments on Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) (RIN 1400-AD70 and RIN 0694-AG32)

Lockheed Martin Corporation (Lockheed Martin) is pleased to submit the following comments in response to the Proposed Rules on Revisions to Definitions in the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR) (See 80 Fed. Reg. 106 at 31525 and 80 Fed. Reg. 106 at 31505) published in the Federal Register on June 3, 2015.

Lockheed Martin commends the Departments of State and Commerce for the continuing effort to harmonize the definitions and terms used in the ITAR and EAR. This will help to prevent conflicting regulatory guidance and ease compliance efforts. It is critical, however, that such efforts do not inadvertently expand controls on common business practices or increase the complexity of the U.S. export control regime. In the effort to have agreement between the ITAR and EAR, we also encourage the Departments to identify ways in which licensing, reporting, and recordkeeping requirements should be reduced. While harmonized definitions will provide needed clarity, it is also imperative to streamline and facilitate the export licensing process to achieve the stated goals of the President's Export Control Reform (ECR) initiative, including focusing controls on the most sensitive transactions and technologies.

I. ITAR §120.10: Technical Data / EAR §772.1: Technology

Installation: As proposed, §120.10(a)(1) controls "installation" as technical data for a defense article. This is inconsistent with the Note to paragraph (a)(2) in the proposed Section §120.9

Defense Service, which explicitly notes that "installation" is performed without the use of technical data. Accordingly, the definition of technical data should exclude "installation" to ensure consistency and clarity.

Recommendation: Remove the term "installation" in the definition of technical data.

Information Controls: §120.10 (a)(5) controls decryption keys, network access codes, or passwords that would allow access to other technical data. Yet, this information is not controlled under the ITAR. Instead, the ITAR appropriately controls the technical data that is to be accessed and does not need to control the means for access. There are several practical reasons to limit controls to the technical data and not the passwords: first, it unnecessarily complicates providing such information to authorized individuals; and second, it could inadvertently control common terms used as passwords in other documents.

Recommendation: Delete (a)(5) from §120.10.

Non-Proprietary Controls: The proposed language of §120.10(b)(1) excludes "non-proprietary" information. By implication, the definition would control "proprietary" information as "Technical Data." There are situations where some information in a general system description is controlled by the author for confidentially and circulation reasons. In this context, all descriptions related to a defense article that contain proprietary information in a general system description would be controlled as Technical Data under the ITAR. This would greatly expand the definition of Technical Data.

Recommendation: Remove "non-proprietary" from §120.10(b)(1).

Removal of "Software": Removing "software" from the definition of "technical data" is appropriate. However, the change has significant implications for existing authorizations and future compliance responsibilities, as the ITAR includes hundreds of references to Technical Data. It is imperative that the removal of "software" does not create gaps in a USML category or inadvertently remove current authorizations included in ITAR exemptions.

Recommendation: Lockheed Martin recommends the Department of State draft a separate proposed rule to provide a clear definition of "software" and an opportunity for the public to comment on where changes are warranted in the ITAR to address the removal of "software" from the definition of "technical data." In addition, we recommend the Department of State provide guidance regarding the completion of license applications to account for the current two options for the "commodity" block in a license application (i.e., DSP-5): "Hardware" or "Technical Data". For cases that include limited defense services, the USG has the capability to authorize the case based on §124.1(a), which defines the standard for approval. Without a modification to the existing forms or a similar provision in the ITAR, the authority and process to issue licenses for software will be unclear.

Technology: The use of the term "technology" to describe information "...result[ing] from..." fundamental research in §734.8 appears to contradict the proposed note that "information that is not 'technology' as defined in the EAR is per se not subject to the EAR."

Recommendation: We recommend replacing the term "technology" in §734.8(a) with the term "information".

II. ITAR §120.11: Public Domain

Ascertaining the Source of Public Information: Once information is in the public domain, it may be impractical, if not impossible, to determine whether technical data has been approved for such release. Paragraph §120.11(b) effectively prevents any U.S. person from assuming that publically available information is not controlled under the ITAR without making separate formal inquiries to the U.S. Government.

For example, Company A presents an article intended for publication in an open source magazine to Department of Defense, Office of Security Review prior to sending the article to the publication. The article contains some information that is Technical Data. The Department of Defense, Office of Security Review approves the article for release with revision. Utilizing 125.4(b)(13), Company A enters the information into the Public Domain. Any Person may access the information in the Public Domain, except that no one other than Company A knows that the information in the article is by definition in the public domain. This not only imposes a significant compliance burden on U.S. companies that must determine whether an appropriate review was conducted, but it also may provide commercial advantages to specific companies that have knowledge of that review and can more efficiently utilize the data in the public domain.

Recommendation: The U.S. Government must revisit the "knowledge" standard with regard to information in the public domain to prevent a cumbersome and impractical review requirement for information already in the public domain.

III. ITAR §120.17 / EAR §734.13: Export

Deemed Exports: The proposed revision to the definition in Sec. 120.17(b) maintains two different "deemed export" license requirements for foreign nationals. The Department of Commerce reviews deemed export applications based on a foreign national's most recent country of citizenship or permanent residency, while the Department of State reviews deemed export based on all countries in which the foreign person has held citizenship or holds permanent residency. The intent of ECR is to harmonize such licensing requirements. Maintaining two standards is contrary to this objective and complicates industry compliance efforts, particularly if a foreign national is the recipient of both ITAR and EAR controlled items.

Recommendation: Lockheed Martin recommends reconciling the two definitions by removing "... and all countries in which the foreign person has held citizenship" and revising 120.17(b) as follows:

> "(b) Any release in the United States of Technical Data or software to a Foreign Person is a deemed export to the Foreign Person's most recent country of citizenship or permanent residency."

Exports of Spacecraft: The proposed definition for "export" appears to exclude the export of spacecraft that are not destined to a D:5 country and do not meet the STA license exception criterion. This could create a scenario where a U.S. person does not require export authority to transfer registration or ownership of a spacecraft to a customer from an STA country if the spacecraft were launched from the United States and the export of the spacecraft is otherwise eligible for export via STA. Additionally it would seem to impose an unnecessary and overly burdensome requirement for additional licensing for typical situations in which US persons were to take control of a satellite overseas for the purpose of initial operational testing and/or in-orbit testing. Such situations should not require a license if the title and ownership of the satellite does not change.

Recommendation: Revise §734.13(a)(3) to read as follows:

§ 734.13 Export.

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

(3) Transferring by a person in the United States of registration or ownership of a spacecraft subject to the EAR to a person in or a national of any other country; or. . .

IV. ITAR §120.46 / EAR §772.1: Required

The newly proposed definition for "Required" as it relates to Technical Data aligns to the existing EAR and Wassenaar Arrangement definitions, which is a positive development. In particular, the addition of Note 2 to §120.46 & §772.1 to align the Technical Data category with the commodity that it represents will increase consistency and aid in making the regulation more intuitive.

Peculiarly Responsible: However, the addition of Note 3 to § 120.46(a) that defines the term "peculiarly responsible" is unnecessary and overbroad. Under the proposed rule, all technical data peculiar to, "the development (including design, modification, and integration design), production (including manufacture, assembly, and integration), operation, installation, maintenance, repair, overhaul, or refurbishing of a defense article" would be controlled unless it satisfies relatively narrow exceptions.

Recommendation: A more effective mechanism for defining "peculiarly responsible" would be to provide an example or language that indicates that not all "technical data" which is required to produce a controlled item is "peculiarly responsible." Rather, only those technologies that are added or combined in such a way to enable achieving or exceeding controlled performance levels, characteristics, or functions should be considered "peculiarly responsible."

V. ITAR §120.52 Activities that are not exports, reexports, or retransfers

The proposed treatment for storage of encrypted data as a non-export activity is a positive regulatory construction. There are, however, several issues that warrant further review:

Transmission through a §126.1 Country: A potential barrier to implementation is the risk that data may be transmitted through, and thereby stored, in a ITAR §126.1/EAR D:5 country or Russia. The challenge is securing the "knowledge" that information entered in a virtual environment (i.e., cloud) is not transiting prohibited terrestrial boundaries. This requires verification of the location of operations and all employees with all potential service providers that support virtual environments, which may not be possible.

"End-to-End" encryption: Information technology security is often a layered approach, and it is possible that multiple levels of encryption, both system or user base, exist requiring decryption keys, network access codes, or passwords for access.

Introduction of Multiple Standards: Multiple standards for encryption introduces complexity (i.e., §120.52 of the ITAR; §734.18 of the EAR, and potentially in the DFAR). Without agreement on a single standard, companies must evaluate the highest standard or attempt to manage information by multiple standards, which diminishes the overall intent to harmonize regulation – increasing both risk and cost.

Jurisdiction: Changing jurisdiction and classification of decryption keys, network access codes, or passwords based on the contents of the encrypted repository is problematic. The current definition of Technical Data continues to provide the consistent standard for what is controlled and for what is a violation under §127.1/§ 764.2, which include the unauthorized visual, oral, written or other inspection of technical data. If the concern is that the four terms used in release do not adequately define the risk for data exfiltration, then the USG should consider broadening the definition of release to capture those actions which identify the transfer without inspection.

Non-Exports: Additionally, providing decryption keys, network access codes, or passwords that would allow access does not constitute a transfer or export since these items are not identified on the USML. If a company is able to forensically prove that these items/data were not transferred or inspected by a foreign party, then it should not constitute an export. The result of investigation and a robust compliance program should be sufficient to review the situation for corrective action and prevent violations.

Double Jeopardy: The broadening of the Technical Data definition to include "decryption keys, network access codes, or passwords" has the potential to characterize a single violation as both the unauthorized release of the technical data and a secondary violation for the release of decryption keys, network access codes, or passwords when an unauthorized foreign party accessed that technical data. The unintended consequence is that the USG enforcement elements now have to account for duplicate violations for a single infringement.

Without addressing these concerns, the proposed regulation will not achieve the goal of defining an acceptable standard for release. To the contrary, the risk and uncertainty may force companies to restrict or eliminate virtual environment (i.e., cloud) as an option for storing data.

Recommendations:

- Reconsider the standard for the release of the decryption keys, network access codes, or passwords as an export in and of itself in sections 120.52 and violation in § 127.1(b)(4).

- Provide further clarification of End-to-End Encryption in light of the fact that it is not uncommon for system or service/third party providers to store decryption keys, network access codes, or passwords for user's accounts in virtual environments.
- Provide a single encryption standard that is identified within the ITAR, EAR, and DFAR.
- Revise or delete §120.10(a)(5)/§ 772.1(a)(5) and §127.1(b)(4)/ § 764.2(l) to revert the definition of Technical Data to the current standard.
- Lastly, include the names of inhabited territories, dependencies, or possessions (American Samoa, Guam, U.S. Virgin Islands, Wake Island) for easy reference in § 120.52(a)(3).

VI. ITAR §120.47: Development

Design Concepts: Design concepts are representative approaches that may or may not meet necessary performance thresholds subject to control under the USML. Concepts have not yet been confirmed through analyses to meet USML control thresholds and are therefore more indicative of general system descriptions than controlled articles.

Recommendation: Delete "design concepts" from the definition of Development.

VII. ITAR §120.48: Production

Production vs. Manufacturing: The addition of the Production definition may expose some of the existing confusion with the term as it is used elsewhere within the ITAR. The new definition of Production is broader than manufacturing and includes manufacturing as only one part of the production process. The §120.21 definition of Manufacturing License Agreement is limited to granting "a foreign person an authorization to manufacture" defense articles. §120.21 does not stipulate that a Manufacturing License Agreement is required if production rights are granted. Likewise, the definition of Technical Assistance Agreement adds more confusion to the situation. In addition, the definition of Production includes assembly, provided that production rights are not transferred. This creates an inconsistency between the definition of Technical Assistance Agreement and the new definition for Production.

The provisions of §124.4(b)(1)-(4) currently apply to Manufacturing License Agreements. The current inclusion of production within the reporting requirement and the broader association to activities beyond manufacturing may cause confusion, potentially increasing the burden by requiring agreement holders to unnecessarily file §124.4(b)(1)-(4) reports for a subset of Technical Assistance Agreements.

Recommendation: Modify §124.4(b) as follows:

§124.4 Deposit of Signed Agreements with the Directorate of Defense Trade Controls
(b) In the case of concluded agreements involving licensed manufacturing of United States origin defense articles outside of the United States, a written statement must accompany filing of the concluded agreement with the Directorate of Defense Trade Controls, which shall include:

(1) The identity of the foreign countries, international organization, or foreign firms involved;
(2) A description and the estimated value of the articles authorized to be manufactured, and an estimate of the quantity of the articles authorized to be produced:
(3) A description of any restrictions on third-party transfers of the foreign manufactured articles; and
(4) If any such agreement does not provide for United States access to and verification of quantities of articles manufactured overseas and their disposition in the foreign country, a description of alternative measures and controls to ensure compliance with restrictions in the agreement on manufactured quantities and third-party transfers.

CONCLUSION

Thank you for the opportunity to provide comments in response to the proposed rules. Lockheed Martin remains committed to supporting the ongoing effort to reform and improve the U.S. export control system. We are confident that the changes recommended above will have a positive impact on our ability to support U.S. national security and foreign policy priorities by harmonizing definitions and aligning compliance standards for U.S. export controls.

If you have any questions related to these comments or would like additional information related to the issues discussed above, please contact Mark Webber, Director, International Trade Policy, Government & Regulatory Affairs at 703-413-5951 or Mark.J.Webber@lmco.com.

For Lockheed Martin,

Mark J. Webber
Director, Government & Regulatory Affairs