LORD Corporation
World Headquarters
111 Lord Drive
Cary, NC 27511-7923
USA

July 31, 2015

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

Email: publiccomments@bis.doc.gov

RE: RIN 0694-AG32

LORD Corporation ("LORD") appreciates the opportunity to review and comment on the proposed rule to harmonize and clarify many of the definitions between the Export Administration Regulations ("EAR") and the International Traffic in Arms Regulations ("ITAR") as part of the ongoing Export Control Reform Initiative.

Our comments and concerns, along with suggested recommendations are as follows:

1. <u>§772.1 – Definitions. "Required" and "Peculiarly Responsible"</u>

   - The effort to include and define 'peculiarly responsible' as part of the harmonization of definitions is appreciated, as we have become accustomed to relating and applying this verbiage when determining if an item is "specially designed". The determination is based upon there being an item that results from development, which has some properties that are unique or peculiarly responsible that enable it to achieve or exceed controlled performance levels, functions or characteristics described in a relevant ECCN or USML paragraph. However, we find it challenging to apply the same process methodology to technical data as proposed in the definitions for "required" and "peculiarly responsible".

   - The insertion of the term "peculiarly responsible" into the first sentence of the "required" definition does not add value or provide clarification.

   - The example provided after the statement *'Such "required" "technology" or "software" may be shared by different products'*, does not seem to be representative of how required technology may be shared, but rather appears to make distinctions between technologies which are "required" and not "required". If this is correct, it is suggested that the statement *'Such "required" "technology" or "software" may be shared by different products'*, be placed elsewhere to avoid confusion.

- The proposed language for defining "peculiarly responsible" seems to be intended to parallel the language contained in "specially designed" as defined in EAR §772.1. However, as currently written, it lacks any parameters or reference points such as 'item', 'development', and 'properties'.

- The proposed definition of "peculiarly responsible" appears to be directed at an item, however, the language of subparagraph (3) uses the term 'information' which we assimilate to technology or technical data.

- In subparagraph (3), the word 'identical' is used as opposed to language that is more aligned with the phrase 'same or equivalent' as used in the definition for "specially designed".

Recommendations:

Following are recommended changes for consideration to the language proposed in §772.1:

"Required"

As applied to technical data, the term ***'****required****'*** *refers to only that portion of technical data that is* ***necessary*** ~~*peculiarly responsible*~~ *for achieving or exceeding the controlled performance levels, characteristics or functions* ***of a relevant ECCN or U.S.. Munitions List paragraph unless:***

1. ***The Department of Commerce has determined otherwise in a commodity classification determination;***
2. ***Reserved;***
3. ***It is technically and functionally equivalent to information used in or with a commodity or software that:***
   (i) Is or was in production (i.e., not in development); and
   (ii) Is EAR99 or described in an ECCN controlled only for Anti-Terrorism (AT) reasons;
4. ***It was or is being developed with "knowledge" that it is or would be for use in or with commodities or software (i) described in an ECCN and (ii) also commodities or software either not 'enumerated' on the CCL or USML (e.g., EAR99 commodities or software) or commodities or software described in an ECCN controlled only for Anti-Terrorism (AT) reasons;***
5. ***It was or is being developed for use in or with general purpose commodities or software (i.e., with no knowledge that it would be for use in or with a particular commodity or type of commodity; or***
6. ***It was or is being developed with "knowledge" that it would be for use in or with commodities or software described (i) in an ECCN controlled for AT-only reasons and also EAR99 commodities or software; or (ii) exclusively for use in or with EAR99 commodities or software.***

For example, assume product "X" is controlled if it operates at or above 400 MHz and is not controlled if it operates below 400 MHz. If production technologies "A", "B", and "C" allow production at no more than 399 MHz, then technologies "A", "B", and "C" are not "required" to produce the controlled product "X". If technologies "A", "B", "C", "D", and "E" are used together, a manufacturer can produce product "X" that operates at or above 400 MHz. In this example, technologies "D" and "E" are "required to make the controlled product and are themselves controlled under the General Technology Note. (See the General Technology Note.)

Such required technical data may be shared by different products.

[continue with the language as written in Notes 1 and 2]

~~"Peculiarly responsible" –~~ [Delete this definition]

2. <u>§734.13 Export</u>

The proposed changes to the definition of 'export' are an improvement from the current language. In an attempt to better parallel the EAR definition of "export" with the ITAR definition provided in §120.17, it is recommended that language be added to acknowledge the fact that the EAR has no equivalent to the ITAR 'defense services'. The addition of such language is in line with this harmonization effort, and would serve as written confirmation that 'defense services' are specific to only the ITAR.

3. <u>§734.18 Activities that are not exports, reexports, or transfers</u>

The addition of this section is a welcomed update and in particular, the inclusion of subparagraph (a)(4) that speaks to sending, taking, or storing "technology" and "software" as well as the supplemental information provided in subparagraphs (b) and (c). The proposed language of (a)(4) and (b) are the particular sections for which we have some concerns.

- 'End-to-end encryption' may be interpreted as more stringent, and in some cases, less stringent than FIPS 140-2, and could be a stand-alone requirement, independent of (iii). For example, if a sufficient 'end-to-end encryption' scheme is employed to protect a given data set, then the additional requirement of a FIPS 140-2 Level 3 certified product to transmit via TLS, such as an IPSec VPN, is redundant. The concern revolves around the differences between 'end-to-end encryption' and FIPS 140-2. To remove ambiguity, clarification on what parameters constitute sufficient 'end-to-end encryption' and when 'end-to-end encryption' versus a validated FIPS 140-1/FIPS 140-2 cryptographic module is required, is needed.

- The definition provided for 'end-to-end encryption' speaks to an originator and an intended recipient, but does not clarify whether an originator means one individual person or one company/entity. In the case of utilizing cloud storage, it would not be unreasonable for companies to need 'many to one' encryption. If the intention of 'originator' is one individual person, companies could incur increased burden and costs by having to obtain individual certificate keys for each employee.

Recommendations:

- Clarification on what parameters constitute sufficient 'end-to-end encryption','
- Clarification on when 'end-to-end encryption' versus a validated FIPS 140-1/FIPS 140-2 cryptographic module is required, is needed (based on recommendation below)
- It is suggested that the language set forth in (a)(4) be considered as follows as well as including a note that provides clarity to the requirements:

(a)(4) Sending, taking or storing "technology" or "software" that is:
(i) Unclassified;
(ii)*~~(iv)~~ Not stored in a country listed in Country Group D:5 (see Supplement No. 1 to part 740 of the EAR) or in the Russian Federation;*
(iii) Secured using cryptographic modules (hardware or "software") compliance with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications, or other similarly effective cryptographic means; and
(iv)*~~(ii)~~ Secured using 'end-to-end encryption'.*

Note to (a)(4): Technology secured using the end-to-end encryption method described in (iv), does not require the additional encryption method described in (iii). However, if technology is secured using the method described in (iii), then the end-to-end encryption method described in (iv) must also be in place.

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

4. <u>§740.9(a)(3)</u>

We are seeking clarification as to whether the exception cited in §740.9(a)(3) may be used to authorize the remote access by a U.S. person or foreign person employee of a U.S. company to technical data maintained on a company server that is located in the United States while they are outside of the United States.

Additional facts:

1) U.S. person or foreign person employee is on travel or temporary assignment outside of the United States;
2) Foreign person employee is authorized to receive the technical data;
3) Access is achieved using a secure/encrypted connection; and
4) The server in which the technical data is stored is secure/encrypted.

If this exemption is permitted to be used to access technical data as described above, it would be helpful to include ‘access’ in this section.

Once again, we appreciate the opportunity to provide comments on these proposed changes. If you have questions or need additional information, please do not hesitate to contact me at 919-342-2378 or at marjorie.alquist@lord.com.

Sincerely yours,

Marjorie L. Alquist
Manager, Global Trade Compliance