Alliance for Network Security

August 3, 2012

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

Re: BIS-2012-0021 and BIS-2012-0022

Dear Sir/Madam:

On June 19, 2012, the Commerce Department's Bureau of Industry and Security (BIS) published a Proposed Rule entitled "Specially Designed Definition" and an Advanced Notice of Proposed Rulemaking entitled "Feasibility of Enumerating 'Specially Designed' Components". These items appeared in 77 FR 36409 and 77 FR 36419, respectively.

The Alliance for Network Security (ANS) is an industry association comprised of Cisco Systems, Google, Hewlett-Packard Company, Hitachi Data Systems Corp., Intel Corp., Juniper Networks, Alcatel-Lucent, McAfee Corp., Microsoft Corp., Novell, Inc., Qualcomm Inc. and Rockwell Automation. For over ten years, ANS has advised the United States and foreign governments with respect to export and import controls on cryptography. We appreciate this opportunity to provide comments with respect to export controls on cryptography under the Export Administration Regulations (EAR).

ANS members support the President's Export Control Reform initiative. ANS members also support the adoption of a common definition of the term "specially designed" for use in relevant sections of the EAR that may be affected by the proposed transfer of certain items from the United States Munitions List of the International Traffic in Arms Regulations (ITAR) if it is done in a way to reduce confusion and capture just the items of interest. However, ANS members do not support the adoption of a common definition of "specially designed" for the balance of the Commerce Control List.

Rather, ANS members believe that the preferred approach is to eliminate or replace the term "specially designed" where it currently appears in the Commerce Control List. ANS members prefer eliminating or replacing the term "specially designed" for the following reasons, among others:

1. The definition published in the Proposed Rule is complicated and imprecise;

2. The definition published in the Proposed Rule has not been adopted by participating member states of the Wassenaar Arrangement or other multilateral regimes;

3. The approach suggested by the ISTAC goes beyond the immediate issue of parts and components, and eliminates or replaces "specially designed" throughout the relevant sections of the Commerce Control list.

In the Advanced Notice of Proposed Rulemaking, BIS indicated particular interest in the use of "specially designed" in the context of Export Control Classification Number 5A002.a. ANS members respectfully suggest that the following definition be given serious consideration:

Systems, equipment, application specific "electronic assemblies", ***cryptographic libraries****, modules,* ***development kits, toolkits, application-specific development kits, chipsets, field programmable logic devices,*** *and integrated circuits* ~~***for "information security"***~~*,* ***providing the means or functions necessary for "information security"*** *as follows:* ~~***and components therefor specially designed for "information security"***~~*:*

Indeed, one might consider replacing the term "specially designed" throughout Category 5, Part 2, by making four types of changes:

1. Remove the term "specially" from the phrase "specially designed and limited" and "specially designed or modified" in the exclusion notes to smart cards and banking and money transactions. "Specially" adds no further distinction for identifying products in light of the use of "designed and limited".

2. Replace the term "specially designed" with the term "providing the means or functions necessary" in 5.A.2.a,, 5.B.2, and 5.D.2. This change would clarify that only components having functionality necessary for "information security" would be classified in 5.A.2.a.

3. Replace the term "specially designed or modified" with the term "providing the means or techniques necessary" in 5.A.2.a.4 to clarify that any hardware providing techniques necesary for reducing eminations of information bearing signals would be classified in 5.A.2.a.4.

4. Replace the phrase "and components therefor specially designed for "information security" in 5.A.2.a with a specific list of components that are controlled in Category 5 Part 2.

The resulting text of Category 5, Part 2 would read as follows:

5. A. 2. "Information security" systems, equipment and components therefor, as follows:

a. Systems, equipment, application specific "electronic assemblies", **cryptographic libraries**, modules, **development kits, toolkits, application-specific development kits, chipsets, field programmable logic devices,** and integrated circuits ~~**for "information security"**~~, **providing the means or functions necessary for "information security"** as follows: ~~**and components therefor specially designed for "information security"**~~:

N.B. *For Global Navigation Satellite Systems (GNSS) receiving equipment containing or employing decryption, see 7.A.5.*

...

5. A. 2. a. 4. ~~**Specially designed or modified to reduce**~~ **Providing the means or techniques necessary for reducing** the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

Note *5.A.2. does not apply to any of the following:*

a. Smart cards and smart card 'readers/writers' as follows:

1. A smart card or an electronically readable personal document (e.g., token coin, e-passport) that meets any of the following:

a. The cryptographic capability is restricted for use in equipment or systems excluded from 5.A.2. by Note 4 in Category 5–Part 2 or entries b. to i. of this Note, and cannot be reprogrammed for any other use; or

b. Having all of the following:

1. It is ~~specially~~ designed and limited to allow protection of 'personal data' stored within;

2. Has been, or can only be, personalized for public or commercial transactions or individual identification; and

3. Where the cryptographic capability is not user-accessible;

Technical Note

'Personal data' includes any data specific to a particular person or entity, such as the amount of money stored and data necessary for authentication.

2. 'Readers/writers' ~~specially~~ designed or modified, and limited~~,~~ for items specified by a.1. of this Note;

Technical Note

'Readers/writers' include equipment that communicates with smart cards or electronically readable documents through a network.

d. Cryptographic equipment ~~specially~~ designed and limited for banking use or 'money transactions';

Technical Note

'Money transactions' in 5.A.2. Note d. includes the collection and settlement of fares or credit functions.

5. B. 2. "Information security" test, inspection and "production" equipment, as follows:

a. Equipment ~~specially designed~~ **providing the means or functions necessary** for the "development" or "production" of equipment specified by 5.A.2. or 5.B.2.b.;

b. Measuring equipment ~~specially designed~~ ~~to evaluate and validate~~ **providing the means or functions necessary for evaluating and validating** the "information security" functions of equipment specified by 5.A.2. or "software" specified by 5.D.2.a. or 5.D.2.c.

5. D. 2. "Software" as follows:

a. "Software" ~~specially designed or modified~~ **providing the means or functions necessary** for the "development", "production" or "use" of equipment specified by 5.A.2. or "software" specified by 5.D.2.c.;

b. "Software" ~~specially designed or modified~~ **providing the means or functions necessary** to support "technology" specified by 5.E.2.;

As the ECR initiative continues, you also may wish to consider whether the term “specially designed” is necessary or desirable in the context of Category XIII on the United States Munitions List (USML) of the ITAR. We note with interest that the State Department’s Directorate for Defense Trade Controls (DDTC) published a proposed rule on May 18, 2012 (77 FR 29575). In this proposed rule, DDTC for the first time introduces the term “specially designed” into the list of information security systems described in Category XIII(b).

ANS members believe that there are two issues deserving of consideration in the context of Category XIII(b). The first is the use of the term “specially designed for military applications”. In this context, “specially designed” appears to retain the “design intent” standard which DDTC professes its interest in replacing. The second is the use of the term “military” to differentiate information security items on the USML from items described on the CCL. The use of “military” in Category XIII(b) fails its intended purpose, because it is essentially self-referential.

A “positive” list of items on the USML might start with a list of items, similar to the following:

- Type 1 classified or controlled cryptographic items endorsed by the National Security Agency (NSA) for securing classified and sensitive U.S. Government information

- Type 2 unclassified cryptographic equipment, assemblies, or components, endorsed by the NSA for the protection of national security information

Other, similar definitions, used in the National Information Assurance Glossary (CNSSI No. 4009) could be employed to develop a comprehensive list of items controlled under Category XIII(b), eliminating the need for the term “specially designed” and the self-referential designator “military”.

In developing such a list, special care must be taken to avoid describing commercial products that are based on international standards from being controlled on the USML. For example, commercial products implementing the Suite B algorithms should not be controlled on the USML.

Respectfully submitted,

Roszel C. Thomsen II
Counsel
Alliance for Network Security