Alliance for Network Security

February 4, 2011

Timothy Mooney
Office of Exporter Services
Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 2705
Washington, DC 20230
ATTB: Notice of Inquiry - CCL

PM/DDTC, SA-1, 12th Floor
Directorate of Defense Trade Controls
Office of Defense Trade Control Policy
ATTN: USML – Positive List
Bureau of Political-Military Affairs
U.S. Department of State
Washington, DC 20522-0112

Re: Request for Public Comments (75 FR 76664 and 75 FR 76935)

Ladies and Gentlemen:

The Alliance for Network Security ("ANS") is the premier trade association representing leading companies engaged in the manufacture and distribution of commercial products incorporating cryptography. ANS is pleased to comment on the proposed rulemakings of the Departments of Commerce and State with respect to the construction of a single, "positive" list of items that currently are subject to control on the United States Munitions List ("USML"), Category XIII(b) of the International Traffic in Arms Regulations ("ITAR", 22 CFR Part 120 et seq.) and on the Commerce Control List ("CCL"), Category 5, Part 2, of the Export Administration Regulations ("EAR", 15 CFR Part 730 et seq.). Because these requests for public comments are closely related, we are addressing these issues in a single submission.

"Positive" List Suggestions

ANS members support the construction of a "positive" list of items controlled. In this regard, we note that Category XIII(b) on the USML of the ITAR is a "design intent" list, rather than a "positive" list of items controlled.

> *(b) Military Information Security Assurance Systems and equipment, cryptographic devices, software, and components specifically designed, developed, modified, adapted, or configured for military applications (including command, control and intelligence applications). This includes*
> *(1) Military cryptographic (including key management) systems, equipment assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, including equipment and software for tracking, telemetry and control (TT&C) encryption and decryption;*
> *(2) Military cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components of software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment;*
> *(3) Military cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components or software;*

(4) Military systems, equipment, assemblies, modules, integrated circuits, components or software providing certified or certifiable multi-level security or user isolation exceeding Evaluation Assurance Level (EAL) 5 of the Security Assurance Evaluation Criteria and software to certify such systems, equipment or software;
(5) Ancillary equipment specifically designed, developed, modified, adapted, or configured for the articles in paragraphs (b)(1), (2), (3), and (4) of this category.

We suggest that this language should be modified to focus on the types of algorithms implemented in such systems. To the best of our knowledge, one important differentiating factor between military and commercial cryptographic products is that military cryptographic products (primarily, if not exclusively) implement algorithms that are classified for reasons of national security. Therefore, restatement of items currently controlled in Category XIII(b) into a "positive" list might provide as follows:

(b) Information Security Assurance Systems and equipment, cryptographic devices, software, and components for military applications (including command, control and intelligence applications implementing cryptographic algorithms that are classified for reasons of national security. This includes (1) Cryptographic (including key management) systems, equipment assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy or confidentiality of information or information systems, including equipment and software for tracking, telemetry and control (TT&C) encryption and decryption;
(2)Cryptographic (including key management) systems, equipment, assemblies, modules, integrated circuits, components of software which have the capability of generating spreading or hopping codes for spread spectrum systems or equipment;
(3) Cryptanalytic systems, equipment, assemblies, modules, integrated circuits, components or software;
(4) Systems, equipment, assemblies, modules, integrated circuits, components or software providing certified or certifiable multi-level security or user isolation exceeding Evaluation Assurance Level (EAL) 5 of the Security Assurance Evaluation Criteria and software to certify such systems, equipment or software;
(5) Ancillary equipment limited to use with the articles in paragraphs (b)(1), (2), (3), and (4) of this category.

The underlines, above, are intended to highlight key text that would differentiate military from dual use items, and is not a word-for-word red-line of the existing language in Category XIII(b).

ANS members also support the construction of a "positive" list of items in Category 5, Part 2 on the CCL of the EAR. In general, such a positive list would be based upon the list of items described in Section 740.17(b)(2) and (b)(3) of the EAR, with modifications.

5. A. 2. Digital systems, equipment, application specific "electronic assemblies", modules, integrated circuits, as follows, and specially designed components therefor:

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

5. A. 2. a. Items having all of the following:

Note 5.A.2.a. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.

1. Items employing a cryptographic algorithm having any of the following:
a. A "symmetric algorithm" key length in excess of 128 bits; or
b. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
1. Factorisation of integers in excess of 1024 bits (e.g., RSA);

2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 1024 bits (e.g., Diffie-Hellman over Z/pZ); or

3. Discrete logarithms in a group other than mentioned in 5.A.2.a.2.b. in excess of 160 bits (e.g., Diffie-Hellman over an elliptic curve); and

Technical Note

For the purposes of 5.A.2.a.1., parity bits are not included in the key length.

2. Being any of the following:

a. "Information security" items having any of the following:

1. Designed, modified, adapted or customized for government end-users or government end-uses; or

2. Providing penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks; or

b. Items designed or modified for "digital computers", "electronic assemblies" or related equipment exceeding the performance levels in 4.A.3.; or

c. Communication equipment providing public safety and other emergency services radio communications and infrastructure services (e.g., mobile devices, terminals, dispatch consoles, gateways, base stations and backhaul equipment implementing Terrestrial Trunked Radio (TETRA) and/or Association of Public-Safety Communications Officials International (APCO) Project 25 (P25) standards); or

d. Network equipment with key lengths exceeding 128 bits for symmetric algorithms having any of the following:

1. An aggregate encrypted WAN, MAN, VPN or backhaul throughput (including communications through wireless network elements such as gateways, mobile switches, and controllers) rate greater than 600 Mbps;

2. A wire (line), cable or fiber optic WAN, MAN or VPN single channel input data rate exceeding 600 Mbps;

3. Transmission over satellite at data rates exceeding 10 Mbps;

4. Media (voice/video/data) encryption or centralized key management supporting more than 250 concurrent encrypted data channels, or encrypted signaling to more than 1,000 endpoints, for digital packet telephony / media (voice/video/data) over internet protocol communications; or

5. Air interface coverage (e.g., through base stations, access points to mesh networks, and bridges) exceeding 1,000 meters, with any of the following:

a. Maximum transmission data rates exceeding 10 Mbps (at operating ranges beyond 1,000 meters); or

b. Maximum number of concurrent full-duplex voice channels exceeding 250.

e. Items described in 5.A.2.a.1 but not otherwise described in 5.A.2.a.2, being any of the following:

a. Chips, chipsets, electronic assemblies and field programmable logic devices;

b. Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);

c. Application-specific hardware or software development kits; or

d. Items that use "non-standard cryptography"; or

f. Providing or performing vulnerability analysis, network forensics, or computer forensics functions having any of the following features or characteristics:

a. Automated network analysis, visualization, or packet inspection for profiling network flow, network user or client behavior, or network structure/topology and adapting in real-time to the operating environment; or

b. Investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data for law enforcement purposes or in a similarly rigorous evidentiary manner; or

g. Systems, equipment, application specific "electronic assemblies", modules and integrated circuits designed or modified to enable an item to achieve or exceed the controlled performance levels for functionality specified by 5.A.2.a. that would not otherwise be enabled.

5. A. 2. b. "Information security" items having any of the following:

1. Designed or modified to perform cryptanalytic functions;

2. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

3. Non-cryptographic information and communications technology (ICT) security systems and devices evaluated to an assurance level exceeding class EAL-6 (evaluation assurance level) of the Common Criteria (CC) or equivalent;

4. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion;

5. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, not specified by 5.A.2.a.2.c.2. including the hopping code for "frequency hopping" systems; or

6. Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:

a. A bandwidth exceeding 500 MHz; or

b. A "fractional bandwidth" of 20% or more; or

7. Designed or modified to use "quantum cryptography".

<u>Technical Note</u>

"Quantum cryptography" is also known as Quantum Key Distribution (QKD).

5. B. Part 2. <u>TEST, INSPECTION AND PRODUCTION EQUIPMENT</u>

…

DEFINITIONS OF TERMS USED IN THESE LISTS

Cat 5P2 "Non-standard cryptography"

Means any implementation of "cryptography" involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published.

Suggestions with Respect to Tiers of Controls

We understand that the Departments of Commerce and State intend to separate the single, "positive" control list into three tiers of items that would create "critical", "substantial" or "significant" military or intelligence advantage to the United States.

We suspect that the items implementing cryptographic algorithms that are classified for reasons of national security might fall into the Tier 1 definition of creating "critical" military or intelligence advantage for the United States. Therefore, we suspect that our reformulated (b)(1) and (b)(2) above might reasonably fall into this category.

We also believe that it would be consistent with the proposed revisions to Category VII published in 75 FR 76930 if the items (b)(3) through (b)(5) were relegated to Tier 2 definition of creating a "substantial" military or intelligence advantage for the United States.

Finally, to align with Wassenaar policy, producing a positive list, and building on the concept of focusing controls on products posing the highest risks, we submit that products and components that by their nature are not susceptible to effective control, and are or will become, widely available or accessible should not be subject to the EAR- dropping out of Tier 3.

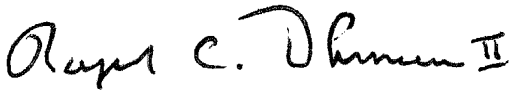
As stated in the National Academy of Sciences report and by Secretary Gates most recently, we should stop trying to control items that by definition cannot be controlled:

> *… an overly broad definition of what should be subject to export control … make[s] it more difficult to focus on those items and technologies that truly need to stay in this country. We need a system that that dispenses with the 95% of the easy cases and lets us concentrate on the remaining 5 percent…*

In light of widespread foreign availability of items listed in Category 5, Part 2 on the CCL of the EAR, we believe that these items should generally fall outside of the Tiered structure of the control list, or in any event should controlled no higher than Tier 3. Such items should be controlled only in the most extenuating circumstances. In this regard, we have attached the Department of Commerce's Information Systems Technical Advisory Committee Report on Foreign Availability.

Thank you very much for this opportunity to provide comments with respect to the controls on cryptographic items listed in Category XIII(b) on the USML of the ITAR and Category 5, Part 2 on the CCL of the EAR.

Sincerely,



Roszel C. Thomsen II