ALSTON&BIRD

WWW.ALSTON.COM

International Trade & Regulatory/Cybersecurity ADVISORY ▪

JUNE 26, 2015

New Export Requirements on the Horizon for Cybersecurity Products and Technologies

A security services provider performs a penetration test on the networks of a foreign corporate client. A developer of an appliance designed to perform network penetration testing sells the device to a customer in another country. Internal corporate network security personnel conduct vulnerability tests of a foreign subsidiary. A multinational organization engages in collaborative cybersecurity research and technology sharing across national borders or with foreign national research personnel in the United States. Companies engage in these types of interactions on a daily basis to help meet ever emerging cyber threats, but under a new regulation proposed by the Department of Commerce's Bureau of Industry Security (BIS), these organizations may now need to obtain export licenses before conducting business and performing their work—even when working with their affiliated companies or with business partners in the most closely allied countries.

In a proposed rule published in the *Federal Register* on May 20, 2015, the BIS has indicated its intent to implement a license requirement for the export, reexport or in-country transfer of certain intrusion and surveillance items (collectively, "cybersecurity items").[1] As industry and technical experts consider the potential scope of the rule, there is uncertainty about the impact of the rule on cybersecurity software developers and device manufacturers and their customers.

Because the proposed rule may reach certain software and hardware solutions that are not apparently intended to be the target, slow down global deployment of these solutions, and raise corporate compliance costs, companies should analyze the full impact of the proposal on their products and services and consider submitting comments. Comments are due July 20, 2015.

[1] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28853 (proposed May 20, 2015) (to be codified in numerous sections and supplements of Subchapter C of Subtitle B, Chapter VII of Title 15 of the Code of Federal Regulations).

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

Background

The new requirement is being implemented pursuant to the United States' commitments under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The Arrangement, which became operational in 1996, is based on a multilateral agreement reached by the founding countries in 1995. Each participating state is responsible for implementing export controls based on annually updated control lists of munitions and dual-use goods and technologies (i.e., having both commercial and potential military applications) through its national legislative or regulatory process. The United States has implemented the export controls required under the Arrangement via the Export Administration Regulations (EAR) and its Commerce Control List (CCL).[2] Cybersecurity items were placed on the Wassenaar Arrangement's list of dual-use goods in 2013. Annual plenary meetings of the participating states regularly result in additions or modifications to the CCL, but this proposal could potentially add controls to a broader swath of hardware, software and technologies than is typical for these annual changes.

Items Affected by the New Controls

The proposed rule would apply new export licensing restrictions to the following items that were added to the list of "dual use" goods under the Wassenaar Arrangement:

> systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; and technology required for the development of intrusion software; [and] Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor.

The descriptions of the cybersecurity items covered are fairly broad; however, the rule would also define several of the key terms used. The final version of these definitions, and the BIS's interpretation of the new provisions, will be critical to determining exactly which items will fall within the scope of the new license requirements.

Items associated with intrusion software

Perhaps the most important term associated with this proposed new set of dual-use items is "intrusion software," which would be defined as:

> "Software"[3] "specially designed"[4] or modified to avoid detection by 'monitoring tools,' or to defeat 'protective countermeasures,' of a computer or network-capable device,[5] and performing any of the following:

[2] *See* 15 C.F.R. 774, Supplement No. 1 (2015).

[3] Defined in 15 C.F.R. § 772.1 as a "collection of one or more 'programs' or 'microprograms' fixed in any tangible medium of expression." *See* 15 C.F.R. § 772.1, Definitions of terms as used in the Export Administration Regulations (EAR).

[4] Whether an item is "specially designed" requires analysis pursuant to the definition of that relatively new term promulgated in connection with Export Control Reform in 15 C.F.R. § 772.1. A full exploration of the analytical framework for determining if an item is specially designed is beyond the scope of this advisory, but it is worth noting that the proposed rule could be the first significant new set of controls to rely heavily upon the specially designed definition, and that the definition, part of the Administration's Export Control Reform effort to establish more "positive" control lists, could leave significant subjectivity when it comes to determining the scope of these cybersecurity controls.

[5] This would include mobile devices and smart meters.

(a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; *or*

(b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

For the purposes of this definition, "monitoring tools" would be defined to include "'software' or hardware devices[] that monitor system behaviors or processes running on a device. This includes antivirus (AV) products, end point security products, Personal Security Products (PSP), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) or firewalls."

Likewise, "protective countermeasures" would be defined to include "techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing."

The definition would also specifically provide that the term "intrusion software" does not include hypervisors, debuggers or software engineering tools, digital rights management software or software designed to be installed by manufacturers, administrators or users for asset tracking or recovery purposes.

The definition is apparently intended to capture a specific group of technologies that are most likely used for hacking purposes, ethical or otherwise. Nonetheless, it is possible that other software products could fall under the scope of the controls, even when not intended for intrusion purposes, if, for example, monitoring software shares certain properties peculiarly responsible for avoiding monitoring software and performs the extraction and modification functions specified in the intrusion software definition. Software developers and manufacturers should therefore be sure to analyze whether their products could fall under the scope of this definition and consider submitting comments seeking modifications of the definitions or increased flexibility in the applicable licensing requirements, as necessary.

In performing this analysis, it is important to note that the scope of the items that would be subject to license requirements is broader than intrusion software itself. Rather, the new requirement would apply to:

1) "systems," "equipment," or "components" [that are] "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software" [proposed ECCN 4A005];

2) "software" "specially designed" or modified for the "development" or "production," of the equipment [proposed amendment to ECCN 4D001];

3) "technology" "required" for the "development" of "intrusion software" [proposed amendment to ECCN 4E001]; and

4) "software" "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software" [proposed ECCN 4D004].

Developers and manufacturers should therefore take into consideration a wide array of items that are associated with intrusion software when considering the potential impact of the new license requirement on their businesses. For example, the proposed amendment to ECCN 4E001 would cover "technology"—defined as "[s]pecific information necessary for the 'development', 'production', or 'use' of a product"[6]—required for the development of intrusion software, which could conceivably cover code compilers or even coding languages or libraries that share key information elements of intrusion software technology even if not specifically intended for use in the development of intrusion software.

Although the BIS has stated that the proposed rule would not control intrusion software itself—only the "command and delivery platforms for generating, operating, delivering, and communicating"[7] with such software—the proposed rule itself notes that technologies that have intrusion software as a component would be within the scope of the controls, such as "network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices." Indeed, because the command platform for operation of intrusion software may be part of the same software bundle as the intrusion software, the proposed rule could have the practical effect of controlling intrusion software itself in many instances. Likewise, if the delivery platform for such software is controlled, the software itself may be effectively controlled. The rule explains that "[t]echnology for the development of intrusion software includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices."

These examples make clear that the new controls may apply to certain white hat security tools, such as penetration testing software or appliances, used by security companies (or by multinational companies on themselves), potentially making the rapid global deployment of such items to respond to cybersecurity threats more difficult for companies to achieve. The proposal also raises questions about the possibility of chilling important security research collaboration across borders or indirectly supporting the development of such research outside the United States.

Items associated with IP network communications surveillance

The proposed rule would also amend ECCN 5A001 to cover "IP network communications surveillance 'systems' or 'equipment', and 'specially designed' components therefor," which meet all of the following criteria:

a) Performing all of the following on a carrier class IP network (*e.g.*, national grade IP backbone):

   i. Analysis at the application layer (*e.g.*, Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498–1));

   ii. Extraction of selected metadata and application content (*e.g.*, voice, video, messages, attachments); *and*

   iii. Indexing of extracted data; *and*

[6] 15 C.F.R. § 772.1.

[7] https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports/deemed-exports-faqs?view=category&id=114#subcat200.

b) Being "specially designed" to carry out all of the following:

i. Execution of searches on the basis of 'hard selectors';[8] *and*

ii. Mapping of the relational network of an individual or of a group of people.

The definition would also specifically provide that the license requirement would not apply to systems or equipment specially designed for marketing purposes, network quality of service or quality of experience. Similar to the proposed definition of "intrusion software," this definition is apparently targeted at network surveillance technology implemented by major telecommunications or broadband carriers and not to systems and equipment used in internal corporate networks, though "carrier class IP network" is not defined in the proposal. As with intrusion software, it is possible that the definition could unintentionally capture items. Anyone who has observed the BIS's administration of the encryption export regulations, which have captured more and more items over the decades as efforts to reform the regulations to keep up with evolving technologies have proved slow and incremental, should understand the need to examine the proposed rule carefully to determine if items they may develop, produce, purchase or deploy now or in the future could fall within the scope of the new license requirements.

Licensing Requirements

The cybersecurity items would require a license prior to export, reexport or transfer (in-country) to (or in) any country other than Canada. In addition to the information required for all classification requests to the BIS, the proposed rule also amends 15 C.F.R. 748, Supplement No. 2, to require that license applicants provide certain technical information, including source code if requested. If the items are designed or modified to use cryptography, as defined by 15 C.F.R. § 772.1, or cryptanalysis, or other information security functionality classified under ECCNs 5A002, 5D002, 5A992.c, 5D992.c or 5E002, as so many commercial information technology and communications software and hardware are, then they continue to be subject to separate and additional registration and review requirements on that basis. The BIS notes in the proposed rule that while remaining subject to existing encryption control requirements, many cybersecurity items will be losing their eligibility for License Exception ENC.

No explanation is offered as to why, given existing encryption controls and government visibility to the exports of such items, such broad new additional restrictions are required. Indeed, a significant concern about the proposed rule is that it denies the use of virtually all license exceptions to cybersecurity items without providing an explanation for doing do. Certainly there are good reasons to allow for license exceptions, for example, for certain intracompany transfers of these cybersecurity items or certain temporary deployments of such items. The BIS notes in the proposed rule that it "anticipates licensing broad authorizations to certain types of end users and destinations…," though it provides no details on such a promised licensing regime and the assurance may prove cold comfort for the loss of any meaningful license exceptions even for transfers to the closest U.S. allies. The licensing burdens could prove to be significant.

[8] "Hard selectors" would be defined as "data or set of data, related to an individual (e.g., family name, given name, email or street address, phone number or group affiliations)." *See* Proposed Rule at 28861.

Under a proposed new licensing policy that would be contained in 15 C.F.R. § 742.6(b)(5), applications for licenses to export, reexport or transfer cybersecurity items would be "reviewed favorably" by the BIS if the items were destined to:

1) A U.S. company or subsidiary not located in a D:1 or E:1 country listed in Supplement No. 1 to 15 C.F.R. 740;

2) Foreign commercial partners[9] located in A:5 countries, which are generally close allies and multiregime members, listed in Supplement No. 1 to 15 C.F.R. 740; or

3) Government end users in Australia, Canada,[10] New Zealand or the United Kingdom, i.e.,
the Five Eyes countries,

and on a case-by-case basis to determine whether the transaction is contrary to the national security or foreign policy interests of the United States, including human rights interests.

In addition, the proposed rule states that "a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities" would be implemented as well.

Conclusion

Even in light of the favorable licensing policy proposed to be added to 15 C.F.R. § 742.6(b)(5), the license requirement could have a significant impact on companies that export, reexport or transfer (in-country)[11] covered cybersecurity items. In light of the considerable uncertainty about the scope of the proposed regulation, software developers, device manufacturers, security testing and analytics service providers, cybersecurity research organizations, and companies that purchase, use and deploy cybersecurity items should consider submitting comments in response to the proposed rule.

[9] A "foreign commercial partner" would be defined as "a foreign-based non-governmental end-user that has a business need to share the proprietary information of the U.S. company and is contractually bound to the U.S. company (e.g., has an established pattern of continuing or recurring contractual relations)." *See* Proposed Rule at 28858.

[10] The rule does not purport to impose licensing requirements on exports, reexports or transfers (in-country) of cybersecurity items to (or in) Canada.

[11] Note that transfer (in-country) is defined as "[t]he shipment, transmission, or release of items subject to the EAR from one person to another person *that occurs outside the United States within a single foreign country*." 15 C.F.R. § 772.1 (emphasis added).

If you would like to receive future ***International Trade & Regulatory Group Advisories*** electronically, please forward your contact information to **trade.advisory@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Kim Peretti
202.239.3720
kimberly.peretti@alston.com

Peter Swire
404.881.4259
peter.swire@alston.com

Jason Waite
202.239.3455
jason.waite@alston.com

Jason Wool
202.239.3809
jason.wool@alston.com

Follow us: On Twitter @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ▪ 1201 West Peachtree Street ▪ Atlanta, Georgia, USA, 30309-3424 ▪ 404.881.7000 ▪ Fax: 404.881.7777
BRUSSELS: Level 20 Bastion Tower ▪ Place du Champ de Mars ▪ B-1050 Brussels, BE ▪ +32 2 550 3700 ▪ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ▪ 101 South Tryon Street ▪ Suite 4000 ▪ Charlotte, North Carolina, USA, 28280-4000 ▪ 704.444.1000 ▪ Fax: 704.444.1111
DALLAS: 2828 North Harwood Street ▪ 18th Floor ▪ Dallas, Texas, USA, 75201 ▪ 214.922.3400 ▪ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ▪ 16th Floor ▪ Los Angeles, California, USA, 90071-3004 ▪ 213.576.1000 ▪ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ▪ 15th Floor ▪ New York, New York, USA, 10016-1387 ▪ 212.210.9400 ▪ Fax: 212.210.9444
RESEARCH TRIANGLE: 4721 Emperor Blvd. ▪ Suite 400 ▪ Durham, North Carolina, USA, 27703-85802 ▪ 919.862.2200 ▪ Fax: 919.862.2260
SILICON VALLEY: 1950 University Avenue ▪ 5th Floor ▪ East Palo Alto, California, USA, 94303-2282 ▪ 650.838.2000 ▪ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ▪ 950 F Street, NW ▪ Washington, DC, USA, 20004-1404 ▪ 202.756.3300 ▪ Fax: 202.756.3333