wiley

ARTICLE

Commerce Department Proposes Expansive New Rule on Cybersecurity Items

May 22, 2015

The Department of Commerce's Bureau of Industry and Security (BIS) published a proposed rule imposing strict controls on the export of certain intrusion and surveillance (or "cybersecurity") items, many of which currently are controlled because of their encryption capabilities or else are designated as EAR99 and are subject to the lowest level of control.[1] The proposed amendments to the Export Administration Regulations (EAR) are designed to implement agreements made in December 2013 by the Wassenaar Arrangement, a group of like-minded countries committed to promoting transparency and responsibility in cross-border transfers of arms and dual-use goods and technologies.

BIS proposes adding new controls in Category 4 of the EAR's Commerce Control List (CCL) to cover hardware and software (along with related technology) specially designed or modified for the generation, operation, or delivery of, or communication with, intrusion software, including network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable products (*e.g.*, mobile devices and smart meters). "Intrusion software" will be defined as software specially designed or modified to avoid detection by monitoring tools (*e.g.*, antivirus products or firewalls) or to defeat protective countermeasures (*i.e.*, techniques designed to ensure the safe execution of code) of a computer or network-capable device. Such software must perform either (1) the extraction of data or information from a computer or network-capable device, or the modification of system or user data; or (2) the modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions. Notably, the definition will not include hypervisors, debuggers, or

Authors

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Practice Areas

Export Controls and Economic Sanctions
International Trade

Software Reverse Engineering (SRE) tools; Digital Rights Management (DRM) software; or software designed to be installed by manufacturers, administrators, or users for the purposes of asset tracking or recovery.

To address the heightened sensitivity surrounding network communication traffic analysis systems that intercept and analyze messages, BIS also plans to add new controls in Category 5, Part 1 of the CCL to cover Internet Protocol (IP) network communications surveillance items that meet certain specified criteria.[2] BIS has stated that its intent is to capture only products that are not specially designed for legitimate network operator functions, and it has excluded items specially designed for marketing, Network Quality of Service (QoS), or Quality of Experience (QoE) purposes from these controls. Items that do not meet all of the criteria for an IP network communications surveillance item generally will be subject to less restrictive controls, except if such items are sold separately with knowledge that they will be combined with other items to make a controlled IP network communications surveillance system.

A license will be required for exports, reexports, and in-country transfers of cybersecurity items to all destinations except Canada. Further, no license exceptions will be available except for exports to or on behalf of the U.S. government. In addition, BIS will have a licensing policy of presumptive denial for items that have or support rootkit (*i.e.*, masking the existence of processes or programs and allowing the user to gain privileged access to a computer) or zero-day exploit (*i.e.*, taking advantage of a security vulnerability before it becomes known to the vendor so that there is no time to fix the problematic code) capabilities.[3]

Cybersecurity items will be classified under the newly defined cybersecurity Export Control Classification Numbers (ECCNs), even if they have encryption functionality. However, such products still must satisfy the EAR's normal encryption rules, including registration, review, and reporting requirements.[4] Encryption products that meet the "cybersecurity" criteria will no longer be eligible for License Exception ENC, a fairly sweeping exception to BIS's licensing requirements. Nonetheless, BIS has indicated that it anticipates granting broad authorizations for exports to certain types of end-users and destinations in an effort to counterbalance the loss of the use of this license exception.

Industry members are encouraged to submit comments on the proposed rule, which are due by July 20, 2015. Of particular interest are comments addressing the number of additional license applications companies will be required to submit, including for products that are currently eligible for license exceptions and products currently classified as EAR99; any negative effects that this rule will have on legitimate vulnerability research, audits, testing, or screening; and any potential detriment that this rule may have on industry's ability to protect networks.

---

[1] *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, 80 Fed. Reg. 28,853 (Dep't Commerce May 20, 2015) (proposed rule, with request for comments).

[2] An IP network communications surveillance item must perform all of the following on a carrier class IP network (*e.g.*, national grade IP backbone): (a) analysis at the application layer (*e.g.*, Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1)), (b) extraction of selected metadata and application content (*e.g.*, voice, video, messages, attachments), and (c) indexing of extracted data. It also must be

specially designed to carry out all of the following: (a) execution of searches on the basis of hard selectors (*i. e.*, data or set of data related to an individual, such as family name, given name, email or street address, phone number, or group affiliations), and (b) mapping of the relational network of an individual or of a group of people.

[3] On the other hand, license applications for controlled cybersecurity items that do not include or support rootkit or zero-day exploit capabilities will be reviewed favorably if destined to a U.S. company or subsidiary not located in Country Group D:1 or E:1, foreign commercial partners located in Country Group A:5, or government end-users in Australia, Canada, New Zealand, or the United Kingdom.

[4] An encryption classification review will be required as a prerequisite to any license application for a cybersecurity item with encryption functionality.