THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 57, No. 22 **June 10, 2015**

Focus

¶ 171

FEATURE COMMENT: Cybersecurity Export Controls—Proposed Changes In U.S. Rules

The Department of Commerce's Bureau of Industry and Security (BIS) May 20 published a proposed U.S. export control rule change for cybersecurity exports. See 80 Fed. Reg. 28853 (May 20, 2015). Affected products include intrusion software, surveillance systems, and related systems, equipment, software and components. The rule would change U.S. cyber export controls and add new licensing requirements for companies developing and selling intrusion and surveillance cyber products. If implemented, the proposed rule likely would result in an effective prohibition on exports to some users.

The proposed rule provides for new and amended export control classification numbers (ECCNs) for "cybersecurity items." ECCNs are used in the Commerce Department rules to determine whether a license is required or a license exception applies for an export to an end user in a particular location for a particular end use.

Currently, cybersecurity items typically are controlled for export through an ECCN based on their cryptographic functionality. Those ECCNs generally allow the use of a license exception, called the encryption or "ENC" license exception, for exports to most locations after meeting certain requirements. The new proposed ECCNs and control regime would disallow the use of most license exceptions, including the ENC license exception, for many of these items.

Export control professionals have been anticipating rulemaking in this area since the 2013 Wassenaar Arrangement agreements added intrusion software and penetration systems to the dual use, multi-lateral export control regime. BIS is seeking comments on the proposed rule, with a deadline of July 20. This FEATURE COMMENT discusses some of the key changes proposed by BIS.

New Proposed Definition of "Intrusion Software"—BIS' proposed rule relies on a new definition of "intrusion software" that is central to understanding the proposed export controls. "Intrusion software" under the proposed rule would include:

> "Software" "specially designed" or modified to avoid detection by "monitoring tools," or to defeat "protective countermeasures," of a computer or network-capable device (including mobile devices and smart meters), and performing any of the following:
>
> (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.

In the proposed rule, "monitoring tools" are software or hardware devices that monitor system behaviors or processes running on a device. These software or hardware devices include antivirus products, end-point security products, personal security products, intrusion detection systems, intrusion prevention systems and firewalls. BIS describes "protective countermeasures" in the proposed rule as techniques designed to ensure the safe execution of code, such as data execution prevention, address space layout randomization or sandboxing.

BIS includes a number of notes within the proposed definition. These notes are helpful in removing certain standard commercial products from the definition. In particular, the proposed definition of "intrusion software" does not include (1) hypervisors, debuggers or software reverse engineering

tools; (2) digital rights management software; or (3) software designed to be installed by manufacturers, administrators or users, for the purposes of asset tracking or recovery.

Proposed New and Amended ECCNs for "Intrusion Software"—Relying on the proposed definition of "intrusion software" summarized above, the proposed rule would add two ECCNs to the Commerce Control List (CCL) for "intrusion software" and related systems, equipment, components and software. These two new ECCNs are:

- 4A005: "systems," "equipment" or "components" for intrusion software, "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software"; and
- 4D004: "software" "specially designed" for the generation, operation or delivery of, or communication with, "intrusion software."

BIS states in the *Federal Register* notice for the proposed rule that these ECCNs include "network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices."

These new ECCNs would have restrictive controls, specifically including listed export controls for national security (NS), regional stability (RS) and anti-terrorism (AT) reasons. Those controls mean, within the BIS regulations, that exports of items falling within the classification of those ECCNs have an export license requirement for all destinations except Canada. No license exceptions (except for certain portions of License Exception GOV) would be available for 4A005 and 4D004 items.

The proposed rule also would change some existing ECCNs. ECCNs currently listed in the CCL that are affected by the "intrusion software" definition and rule change include 4D001, which would cover "development" and "production" intrusion software, and 4E001 which would cover "technology" "required" for the "development" of intrusion software. In its *Federal Registe*r notice seeking comments on the proposed rule, BIS states that technology in this case would include "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices." Like the proposed ECCNs 4A005 and 4D004, these amended ECCNs would not be eligible for the use of license exceptions, including License Exception Technology and Software Under Restriction or Strategic Trade Authorization.

Proposed Network Communications Surveillance Systems ECCN—In addition to the changes noted above, BIS proposes to add Internet Protocol network communication surveillance systems as "cybersecurity items" in ECCN 5A001.j. These surveillance systems include systems that intercept and analyze messages to produce personal, human and social information from network communications traffic. BIS would exclude from ECCN 5A001.j systems or equipment specially designed for a marketing purpose, network quality of services, or quality of experience.

Similar to ECCNs 4A005 and 4D004 for "intrusion software," ECCN 5A001.j. would include controls for NS, RS and AT (all Column 1) reasons. The result of those controls is the requirement of a license for all exports and reexports except those destined for Canada. In addition, similar to the "intrusion software" ECCNs, 5A001.j would not be eligible for license exceptions, except for certain provisions of GOV.

Proposed Ongoing Registration, Review and Reporting Requirements for Cryptographic Items—As noted above, "cybersecurity items" would not be eligible for the encryption-related license exception "ENC." They also would no longer be classified according to their information security functionality (e.g., in ECCNs 5A002, 5D002 or 5E002). However, these cybersecurity items—including intrusion software and network communication surveillance systems—would still have the same information security registration, review and reporting requirements that currently apply to encryption items.

Relevant new and amended ECCNs for cybersecurity items (discussed above) include a proposed note that would require the registration, review and reporting aspects of now-existing §§ 740.17, 742.15(b) and 748.3(d), including with BIS and the ENC encryption request coordinator, for these cybersecurity items. Currently, companies customarily seek to meet these requirements to qualify for ENC license exception or mass-market treatment, i.e., in order to avoid the need to obtain a license for qualifying exports. Under the proposed rule, these registration, review and reporting requirements would continue, even though the ENC license exception and favorable mass-market treatment for encryption products would not be available.

Proposed Export Licenses for Cybersecurity Items—Although licenses would be required to most destinations, BIS states in its May 20 release that, under the proposed rule, it would review favorably license requests to certain destinations. These

favored destinations include (1) U.S. companies or subsidiaries outside Country Group D:1 (which includes China, Russia and Vietnam, among others) or E:1 countries (Cuba, Iran, North Korea, Sudan and Syria); (2) commercial partners in Country Group A:5 (which includes many European countries, plus Australia, Japan, South Korea and Argentina, among others); and (3) government end users in Australia, Canada, New Zealand and the United Kingdom. BIS states that there would be a presumption of denial of licenses for items that have or support rootkit or zero-day exploit capabilities. BIS also proposes to review items for licensing based on their information security or cryptographic functionality.

BIS proposes adding new license application rules for cybersecurity items. Specifically, license applications for cybersecurity items would have to fulfill new requirements under the proposed rule, including the submission of particular technical information about the products and, upon request, copies of sections of source code and other software implementing or invoking cybersecurity functionality.

The proposed rule's change for intrusion software and surveillance systems would result in new licensing requirements for some products that currently qualify for ENC or other license exceptions. Licenses will be particularly hard to come by for government end users outside of a few English-speaking countries.

Companies that develop, produce, test and market intrusion software and related cybersecurity items will want to consider carefully comments on the potential impact of the rule on their business, including whether the proposed implementation of the new licensing rules and ineligibility for license exceptions will impose unmanageable burdens. Companies should pay particular attention to their exports outside of the favorable countries discussed in the BIS release. Companies operating in the cybersecurity field will also want to comment on whether certain aspects of the proposed rule could increase the security vulnerabilities of U.S. or multinational companies and U.S. allies, and whether they may hamper vulnerability research and testing, and the ability to protect commercial and government networks.

✦

This FEATURE COMMENT was written for THE GOVERNMENT CONTRACTOR by Alex Baj, Stewart Baker, Jack Hayes, Andy Irwin, Ed Krauland, Meredith Rathbone, and Michael Vatis of Steptoe & Johnson LLP. Baj, Hayes, Krauland and Rathbone are members of the Firm's International Regulation and Compliance Practice; Baker and Vatis its National and Homeland Security Practice; and Irwin its International Regulation and Compliance and Government Contracts Practices.

