Trade Compliance Flash: Commerce Department Issues Rule to Impose Export Controls on Certain Cybersecurity Related Hardware, Software, and Technology

International Alert
12.07.2021

On October 21, 2021, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) issued an interim final rule to amend the Export Administration Regulations (EAR) to control certain types of cybersecurity items. The rule will go into effect on January 19, 2022. Notably, this rule will impose export controls on certain types of "intrusion software" and related items, such as IP network communications surveillance systems. BIS explains that these items need to be controlled for export because they could be used for malicious purposes.

This rule implements an international agreement from 2013 with the Wassenaar Arrangement, a multilateral export control regime consisting of 42 countries. In 2015, BIS proposed implementing those revisions, but it was met with stiff resistance by industry and Congress, which were concerned with the scope and impact of the proposed rule. In response, BIS returned to Wassenaar to renegotiate these controls and which were approved in 2017.

Consequently, this rule differs from the proposed version as it: (1) uses the term "command and control" to better target some of the items that should be controlled, (2) excludes "technology" that is exchanged for "vulnerability disclosure" or "cyber incident response," and (3) excludes software that is designed for and limited to providing basic software updates and upgrades. Additionally, the EAR will add a new license exception for such items, called Authorized Cybersecurity Exports (ACE). BIS believes that the result of this rule on the regulated community should be minimal.

Additionally, BIS recently published a 16-page document with responses to 29 frequently asked questions that provides additional guidance.

Specific Revisions

This rule will add several controls to the Commerce Control List, specifically within Category 4 and Category 5, Part 1. That said, the EAR is being amended to make clear that certain controls within Category 5, Part 2 (*e.g.*, Export Control Classification Number (ECCN) 5A002.a) supersede these new controls when appropriate. In addition, if an item is controlled for multiple reasons that include for Surreptitious Listening (SL) reasons, then the relevant SL control applies, because it is the most restrictive. The following is a high-level overview of these revisions.

Commerce Control List

ECCN 4A005 is added to control "systems," "equipment," and "components" therefor, "specially designed" or modified for the generation, command and control, or delivery of "intrusion software." ECCN 4D004 is added to control: "software" "specially designed" or modified for the generation, command and control, or delivery of "intrusion software." ECCN 4E001.c is added to control "technology" for the "development" of "intrusion software." Consequently, while the hardware and software ECCNs require more than "intrusion software" for those controls to apply, development technology for "intrusion software" is sufficient to be captured by 4E001.c. These entries are controlled for national security (NS1) and anti-terrorism (AT1) reasons and the ACE license exception may be applicable.

These entries refer to the EAR's definition of "intrusion software":

> "Software" specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures,' of a computer or network-capable device, and performing any of the following:
>
> (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.
>
> Note 1 to "Intrusion software" definition: "Intrusion software" does not include any of the following: Hypervisors, debuggers or 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.
>
> Note 2 to "Intrusion software" definition: Network-capable devices include mobile devices and smart meters.
>
> Technical note 1 to "Intrusion software" definition: 'Monitoring tools': "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.
>
> Technical note 2 to "Intrusion software" definition: 'Protective countermeasures': techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

BIS is also amending ECCN 4D001.a to include "software" "specially designed" or modified for the "development" or "production" of equipment or "software" controlled by ECCN 4A005.

Similarly, according to the General Technology Note, ECCN 4E001.a now covers "technology" for the "development," "production," or "use" of equipment or "software" controlled by 4A005, 4D001, and 4D004. Those "technology" controls do not apply to "vulnerability disclosure" or "cyber incident response." The EAR is being amended to define those new terms as:

> Cyber incident response (§ 740.22, Cat 4) means the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cybersecurity incident.
>
> Vulnerability disclosure (§ 740.22, Cat 4) means the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.

ECCN 5A001.j is added to control certain types of IP network communications surveillance systems or equipment and "specially designed" components therefor. As such, ECCNs 5B001, 5D001, and 5E001 will now cover related items, software, and technology for those 5A001.j-controlled items. These entries are controlled for national security reasons and for anti-terrorism

reasons, which generally requires a license unless an exception applies. In addition, BIS authorizes certain IP network surveillance products under license exception ACE, if the circumstances permit.

New License Exception

To address the substantial concerns raised in 2015, the EAR will add a new license exception under section 740.22 called ACE. Subject to its terms and conditions, that license exception will authorize the export, reexport, and transfer (in-country), including deemed exports and reexports, of certain identified cybersecurity items that are identified within paragraph (b) of the license exception (and which covers the ECCNs discussed above). Those items include the IP network communications surveillance items controlled by ECCN 5A001.j, including the relevant software and technology controls. License exception ACE also defines "digital artifacts" and provides definitions for "favorable treatment cybersecurity end user" and "government end user."

Significantly, paragraph (c) provides numerous destination and end user restrictions. If the activity does not involve a Country Group D or E country, such as China or Russia, then these restrictions do not apply. For example, the license exception cannot be used for a destination listed in Country Group E:1 or E:2. It also cannot be used for a government end user — as that term is broadly defined within paragraph (b) — to any country listed in Country Group D:1 through D:5, though it has some further exceptions from that restriction. It also restricts license exception ACE from non-government end users located in Country Group D, but then does not apply that restriction if the activities involve certain "cybersecurity items" to a "favorable treatment cybersecurity end user," concern "vulnerability disclosure" or "cyber incident response," or are deemed exports.

Finally, paragraph (c) provides an end use restriction that broadly applies to any end user, where the person using the exception "'knows' or has 'reason to know' at the time of activity that the 'cybersecurity item' will be used to affect the confidentiality, integrity or availability of information or information systems, without authorization by the owner, operator or administrator of the information system (including the information and processes within such systems)."

Next Steps

The interim final rule is lengthy and includes several requirements, caveats, revisions, and conditions that should be carefully reviewed and considered, particularly when applying the new rules to specific facts and circumstances. Companies and organizations should review the rule now to determine how it will apply, including the applicability of license exception ACE. They should also consult BIS' published FAQs.

For more information, please contact:

Timothy P. O'Toole, totoole@milchev.com, 202-626-5552

Christopher Stagg, cstagg@milchev.com, 202-626-5931

Caroline J. Watson, cwatson@milchev.com, 202-626-6083

Manuel Levitt, mlevitt@milchev.com, 202-626-5921

Mary H. Mikhaeel, mmikhaeel@milchev.com, 202-626-5909

Brian J. Fleming*

**Former Miller & Chevalier attorney*
