Crowell

CLIENT ALERT

Close of Comments on Commerce Cyber Rule

December 6, 2021

Today, December 6th, is the deadline to file comments on the Department of Commerce's Bureau of Industry and Security's (BIS) interim final rule introducing export controls over cybersecurity items. The rule was issued on October 21st and broadly speaking covers intrusion software and internet protocol (IP) network communication surveillance that software is "subject to the Export Administration Regulations (EAR)," i.e., is either exported from the United States or is developed and exported from abroad with more than a minimal percentage of U.S.-origin content.[i]

The purpose of these new controls is to "deter the spread of certain technologies that can be used for malicious activities that threaten cybersecurity and human rights."[ii] As ransomware incidents have continued rise year over year, a common denominator among incidents has been threat actors leveraging professionally-created intrusion simulation software, such as Cobalt Strike, to establish persistence in a network, move laterally, and ultimately deliver an undetectable payload that encrypts the victim's data. Once safely inside a victim's network using the intrusion software, threat actors often similarly abuse network surveillance software to monitor communications and extract sensitive data from an organization. This technology has been used to monitor dissidents, journalists, and at-risk minority populations and many authoritarian regimes have routinely abused commercial surveillance software to perpetuate human rights abuses.

Given this context, to appropriately tailor the rule, BIS imposed a license requirement and also creates a new license exception for cyber security products called "Authorized Cybersecurity Exports (ACE). However, the applicability of ACE is very fact dependent. The rule is further explained by a set of FAQs BIS published on its website November 12, 2021.

Background

This rule implements changes adopted by the Wassenaar Arrangement, a multilateral export control regime with 42 participating states that agree on a unified list of military and dual use items that are then subjected to export controls by the local laws of participating states.

The Wassenaar Arrangement initially implemented controls on cybersecurity items in 2013. BIS published a proposed rule in 2015 to implement these rules but was met by extensive industry pushback. Industry was concerned that the rule was overbroad, imposed unnecessarily burdensome license requirements, and would cripple the development of cyber research. In response, BIS renegotiated with the Wassenaar Arrangement and the Wassenaar Arrangement updated the proposed controls in 2017. This interim final rule brings the U.S. in line with the rest of the Wassenaar Arrangement participating member states.

What is Controlled (and What is Carved Out)

The primary categories of cybersecurity items subject to controls are intrusion software IP network communication and surveillance. To regulate these items, BIS created new export control classification numbers (ECCNs). ECCNs are designations

used to identify items on the Commerce Control List (CCL), one of the lists used to determine the necessity of an export license from BIS.

Intrusion Software

Intrusion Software is defined as 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:

- The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
- The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.

ECCNs that were added or modified to cover intrusion software include

- 4A005: to cover "systems, equipment and components specially designed or modified for the generation, command and control, or delivery of intrusion software."
- 4D004: to cover software specially designed or modified for the generation, command and control, or delivery of intrusion software.
    - However, software specifically designed and limited to providing basic updates and upgrades is excluded from this definition.
- 4E001.c: to cover technology for the development of intrusion software.
- 4E001.a: to cover technology for the development, production, or use of equipment or software controlled by certain ECCNS in 4A.
    - However, software designed for vulnerability disclosure and cyber incident response is excluded for certain end users. The new rule defines "vulnerability disclosure" and "cyber incident response."

IP Network Communications

ECCN 5A001.j was added to cover IP network communications surveillance systems or equipment. In order to fall under the ECCN the item must meet all of the following:

- Performing all of the following on a carrier class IP network (*e.g.,* national grade IP backbone):
    - Analysis at the application layer (Layer 7 of the Open Systems Interconnection (OSI) model);
    - Extraction of selected metadata and application content (*e.g.,* voice, video, messages, attachments); *and*
    - Indexing of extracted data; *and*
- Being "specially designed" to carry out all of the following:
    - Execution of searches on the basis of "hard selectors"; *and*
    - Mapping of the relational network of an individual or of a group of people.

License Exception: ACE

License exceptions allow items that normally require a BIS license to be exported reexported, or transferred without going through the licensing process. The interim final rule creates a new license exception, Authorized Cybersecurity Exports (ACE). Generally, ACE allows for the export, reexport, and transfer of "cyber security items" for certain end uses and end users.

There are several end uses and end users excluded from license exception ACE; a a license would be needed for these transactions:

End Uses Not Eligible for ACE

ACE can never be used if the exporter, reexporter, or transferrer knows or has reason to know at the time of the transaction 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"

End Users Not Eligible for ACE

ACE can never be used for Cuba, Iran, North Korea, or Syria[iii]

The next set of end user restrictions turns on the applicability of two types of users.

- "*Government end user*" as defined for this section of the EAR which means "a national, regional or local department, agency or entity that provides any governmental function or service, including international governmental organizations, government operated research institutions, and entities and individuals who are acting on behalf of such an entity. This term includes retail or wholesale firms engaged in the manufacture, distribution, or provision of items or services, controlled on the Wassenaar Arrangement Munitions List."
- "*Favorable Treatment Cybersecurity End User*" which includes: U.S. subsidiaries, providers of banking and other financial services, insurance companies, and civil health and medical institutions providing medical treatment or otherwise conducting the practice of medicine, including medical research.

ACE cannot be used for government end users in "Group D" countries[iv] such as Russia and China.[v] There is an exception to the exclusion. Certain types of cybersecurity products can be exported, reexported, or transferred to certain end users for certain end uses in these Group D countries only: Cyprus, Israel and Taiwan.

ACE cannot be used for non-government end users in countries listed in group D:1 (which is controlled for national security reasons) or group D:5 (which includes U.S. arms embargoed countries). These groups also include China and Russia. Two exceptions to this exclusion are

- Favorable Treatment Cybersecurity End Users (defined above) can still use ACE for certain cybersecurity items.
- When cybersecurity items are being exported for use in a vulnerability disclosure or cyber incident response (as discussed above) they may use ACE.

Notable FAQS:

The EAR 'cyber rule' FAQs recently published answer several important questions, such as:

- "Published" technologies are not "subject to the EAR" and are not subject to the new controls. "Published" and open source are not necessarily the same thing. BIS considers software "published" if it is made available to the public without further restrictions on dissemination. "Open source" may still subject those obtaining the source code to further restrictions on the dissemination of that source code. There are further requirements for software with encryption functionality to be considered "published," including a requirement to supply the source code to BIS.
- Newly-identified vulnerabilities, also known as "zero day" exploits, in and of themselves are not affected by the rule; however, a vulnerability that is bundled with a payload that includes certain command and control capabilities very well could be covered by the rule.
- Intra-company transfers of surveillance technology to monitor a company's own networks overseas, in most situations, would not require an export license.
- Whether a license is required may in fact depend on the context for which the technologies sought to be exported are going to be used – license exceptions exist when technologies will be used for vulnerability disclosure or incident response.
- License exemptions do not apply whenever an exporter would have reason to believe that the technology at issue will be misused to eavesdrop, steal, alter, or destroy another's data without authorization.

Take Away

Although BIS announced that it was seeking to minimize the impact, the rule will directly affect penetration testers, red teams, cybersecurity researchers, and software companies, with knock-on effects throughout the cybersecurity supply chain because it will affect the way certain products are sourced and the methodologies used to assess and measure cybersecurity risk and compliance. Any US company that exports software and technologies "subject to the EAR" must carefully review these new requirements to determine whether any products or services may be covered by these new rules. Similarly, companies abroad that rely on cybersecurity software and technologies from the United States, should also analyze the new rules to ensure that critical services are not interrupted or discontinued.

---

[i] Definition of cybersecurity items are any item defined in § 740.22 of the EAR as ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005, 4D001.a (for 4A005 or 4D004) or 4D004), 4E001.c, 5A001.j, 5B001.a (for 5A001.j), 5D001.a (for 5A001.j), 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)), and 5E001.a (for 5A001.j or 5D001.a (for 5A001.j)).

[ii] Except of statement from U.S. Secretary of Commerce Gina M. Raimondo.

[iii] Country groups E:1 and E:2

[iv] The list of countries in Group D can be found here. https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-country-groups-1/file

[v] Country groups D:1 and D:5.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kate M. Growley, CIPP/G, CIPP/US
Partner – Washington, D.C.
Phone: +1.202.624.2698
Email: kgrowley@crowell.com

Alexander Urbelis
Senior Counsel – New York
Phone: +1.212.895.4254
Email: aurbelis@crowell.com

Robert Clifton Burns
Senior Counsel – Washington, D.C.
Phone: +1.202.688.3448
Email: cburns@crowell.com

Chandler S. Leonard
Associate – Washington, D.C.
Phone: +1.202.624.2905
Email: cleonard@crowell.com

Rachel Schumacher
Associate
Email: RSchumacher@crowell.com