wiley

ALERT

Commerce Department Issues Long-Awaited Rule on Cybersecurity, Hacking Tools

October 22, 2021

On October 21, 2021, the Department of Commerce's Bureau of Industry and Security (BIS) published a long-awaited interim final rule that establishes controls on certain cybersecurity items designed to curtail exports of hacking tools to China, Russia, and other countries that may use such items for malicious purposes. The interim rule also creates a new license exception for Authorized Cybersecurity Exports (ACE). The purpose of the interim rule, according to the Commerce Department, is to "help ensure that U.S. companies are not fueling authoritarian practices," such as the use of technology to abuse human rights or conduct other nefarious cyber activities.

The rule follows a spate of hacking incidents and stems from a controversial BIS 2015 proposal that was criticized by industry as potentially undermining cybersecurity research and innovation. BIS seeks to address these practical concerns in the interim rule and is requesting public comments on the projected impact of the rule on industry and the cybersecurity community. The interim rule goes into effect on **January 19, 2022**. Comments on the rule are due by **December 6, 2021**.

Background: The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar Arrangement) is a multilateral export control regime in which 42 participating countries, including the United States, agree to maintain controls on exports of certain sensitive dual-use (*i.e.*, military and civilian uses) goods and technologies and certain munitions items. In 2013, the Wassenaar Arrangement added specific cybersecurity items for control, as well as a definition for "intrusion software," to its list of items that should be subject to export controls in member countries. In May 2015, BIS published a proposed rule

Authors

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Practice Areas

Cybersecurity
Export Controls and Economic Sanctions
International Trade
National Security

describing how it would implement these controls in the Export Administration Regulations (EAR) and requested public comments. After hearing from the private sector, Congress, and academia of potential unintended, adverse consequences of the rule on cybersecurity research and incident response, including on defensive capabilities, the United States returned to the negotiating table. In response, in 2017, the Wassenaar Arrangement published several changes to the initial controls, and this interim rule seeks to implement those modified controls.

Scope of the New Controls: The new rule differs from the 2015 proposal in several ways that aim to limit its scope. Specifically, it does not seek to control certain technology exchanged for vulnerability disclosure or cyber incident response, it adds "command and control" language to better target tools that can be used maliciously, and it also excludes from control certain products designed and limited to providing basic software updates and upgrades. Provided below is a brief summary of the new cybersecurity item controls:

- **New ECCNs Related to "Intrusion Software:"** The interim rule creates three new ECCNs related to the generation, command and control, or delivery of "intrusion software" – 4A005 (systems, equipment, and components), 4D004 (software), and 4E001.c (technology).
  - The EAR defines "intrusion software" as software specially designed or modified to avoid detection by monitoring tools or to defeat protective countermeasures, of a computer or network-capable device by either extracting or modifying data or information on a computer or modifying the standard execution path of a program or process to execute external instructions.
  - The software controls in ECCN 4D004 will not control software specially designed and limited to providing updates or upgrades, provided that the updates or upgrades operate only with the authorization of the system owner/administrator and that, once the update/upgrade is complete, the underlying software does not qualify as intrusion software or software meeting the criteria of ECCN 4D004.
  - Additionally, to address prior concerns raised by industry and the cybersecurity community, the related technology controls expressly do not apply to "vulnerability disclosure" or "cyber incident response." "Vulnerability disclosure" is defined as "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." "Cyber incident response" is defined as "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."
- **New ECCN for "IP network communications surveillance systems or equipment:"** The interim rule creates a new ECCN 5A001.j for IP network communications surveillance systems and equipment and specially designed components that perform, on a national grade IP backbone, analysis at the application layer, extraction of selected metadata and application content (*e.g.,* voice, video, messages, attachments), and indexing of extracted data; and are specially designed to execute searches based on hard selectors and map relational networks of an individual or group of people. This new control will not apply to systems or equipment specially designed for marketing purposes,

network quality of service, or quality of experience.

- **Corresponding/related changes:** BIS also made other corresponding and related changes, including adding notes to the regulations to assist exporters in determining the correct classification of their cyber products. To the extent an end item or executable software meeting the description of a cybersecurity item also includes controlled encryption or information security functionality, these latter controls in Category 5, Part 2 of the EAR's Commerce Control List (CCL) will prevail. Similarly, if a product is controlled for Surreptitious Listening (SL) reasons—one of the most restrictive controls on the CCL—then the SL control will trump both the cyber and encryption controls.

New License Exception ACE: Although the newly-added cybersecurity items will be subject to stringent National Security (NS) export licensing requirements, the interim rule provides a broad license exception that is aimed at avoiding impediments to legitimate cybersecurity research and incident response activities. With the exception of sanctioned countries/regions (*i.e.*, destinations listed in Country Groups E:1 and E:2), the license exception allows for the export, reexport, and transfer of cybersecurity items to most destinations without the need to apply for a specific license from BIS. However, it includes two types of end user restrictions as well as one end use restriction, as described below:

- **Government End User Restriction:** License Exception ACE includes restrictions for government end users in any country listed in Country Group D:1, D:2, D:3, D:4, or D:5 in the EAR. However, the government end user restriction does not apply to exports to Cyprus, Israel, and Taiwan of (1) digital artifacts (*i.e.*, software or technology found on an information system and showing activity pertaining to the use or compromise of, or other effects on, that information system) related to a cybersecurity incident involving information systems owned or operated by a "favorable treatment cybersecurity end user" or to a police or judicial bodies for the purposes of criminal or civil investigations of such cybersecurity incidents; or (2) cybersecurity items provided to national computer security incident response teams for the purposes of responding to cybersecurity incidents, vulnerability disclosures, or criminal investigation or prosecution of cybersecurity incidents. Note that a "favorable treatment cybersecurity end user" includes: (1) U.S. subsidiaries; (2) banks or other financial service providers (3) insurance companies; and (4) civil health and medical institutions.
- **Non-Government End User Restriction:** The new license exception also includes an end user restriction applicable to non-government end users located in a country listed in Country Group D:1 or D:5, including China and Russia. However, this restriction does not apply to cybersecurity items provided to any "favorable treatment cybersecurity end user" or to vulnerability disclosure or cyber incident response. Nor does this restriction extend to "deemed exports," *i.e.*, disclosures of controlled technology or source code to a foreign national of a D:1 or D:5 country that occur in the United States.
- **End Use Restriction:** The license exception also will not apply if the exporter knows or has reason to know 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 system (including the information and processes within such systems).

What this means for the industry: The interim rule is more targeted and precise in its controls than the original proposal. It seeks to strike a balance between aligning with our allies to ensure that hacking tools are not used for malicious purposes, while also encouraging defensive cybersecurity activities. Nonetheless, industry members are encouraged to carefully review the new rule and definitions and submit comments to BIS to the extent that the new controls may stymie or even cripple critical innovation, research, and other activities of the U.S. cybersecurity industry.

Wiley has unparalleled experience assisting clients to navigate BIS's controls. Should you have any questions, please do not hesitate to contact one of the attorneys listed on this alert.

Nicole Hager, a Law Clerk at Wiley Rein LLP, contributed to this alert.