The Computer & Internet Lawyer

Volume 39 ▲ Number 2 ▲ February 2022

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Being a White-Hat Hacker Just Got Tougher: U.S. Commerce Department Issues New Cybersecurity Export Controls on Intrusion and Surveillance Tools

By Melissa Duffy, James Koenig, Tyler G. Newby, David Feder and Jean Chang

The U.S. Department of Commerce's Bureau of Industry and Security ("BIS") has published new export controls[1] on certain cybersecurity items that ban the export or resale of hacking tools to authoritarian regimes, and it created a new license exception for those items.

The new regulations aim at tightening export controls on cybersecurity tools, including intrusion software, internet protocol ("IP") network communications surveillance, and related technology that could be used by threat actors to conduct malicious cyber activities and surveillance.

Melissa Duffy, a partner in Fenwick & West LLP, focuses her practice on a broad range of international trade matters. **James Koenig** and **Tyler G. Newby** are partners in Fenwick and co-chair the firm's privacy and cybersecurity practice. **David Feder**, counsel to the firm, represents technology and life sciences companies in commercial litigation matters. **Jean Chang** is an associate at the firm. The authors may be contacted at *mduffy@fenwick.com*, *jkoenig@fenwick.com*, *tnewby@fenwick.com*, *dfeder@fenwick.com* and *jchang@fenwick.com*, respectively.

BIS requested public comments for potential revision before the effective date of the interim rule. In December, BIS published 12 sets of comments from industry, summarized below.

BIS contends that these controls are narrowly drawn, focusing on specific cyber-intrusion and network surveillance equipment, software and technology, and, when combined with the new license exception, that they should have limited impact. The rule adopts cybersecurity controls previously agreed to at the multilateral Wassenaar Arrangement, bringing U.S. controls into alignment with those already adopted by the European Union and other jurisdictions.

However, network infrastructure manufacturers, cybersecurity software and service providers, IT forensics firms, bug bounty programs, and those engaged in vulnerability testing and research may feel the impact of the rule.

Further, exports to national security concern countries such as China and Russia will be highly restricted, and companies dealing with Cypress, Israel and Taiwan will have to navigate new restrictions, notwithstanding those countries' stronger relationships with the U.S.

Background

These new cybersecurity export controls close the loop on a proposed rule, issued by BIS in 2015, to implement multilateral controls agreed to by the Wassenaar Arrangement in 2013.

After issuing the proposed rule, BIS received overwhelming feedback from industry, including hundreds of public comments on the record, criticizing the effort as having severe negative unintended consequences on legitimate cross-border cybersecurity work. General themes from the criticism included that the controls were overly broad in the defined scope of tools and technologies, that they imposed a cumbersome export licensing requirement that would impede the work of white-hat hackers and bug bounty program participants, and that the restrictions on the development of intrusion software would inhibit international cybersecurity research.

BIS renegotiated the controls at Wassenaar to address these concerns, leading to the multilateral adoption of revised controls in 2017. This new rule from BIS implements that most recent version.

Overview of New Cybersecurity Controls

BIS is establishing new controls on certain cybersecurity items for national security ("NS") and anti-terrorism ("AT") s, through the creation of new export control classification numbers ("ECCNs") on the Commerce Control List ("CCL") and definitions in the Export Administration Regulations ("EAR").

Additionally, BIS is creating a new license exception for Authorized Cybersecurity Exports ("ACE"), authorizing export transactions involving these newly controlled items to most destinations while restricting exports to a national security concern group of countries.

A high-level summary of the new controls follows.

Intrusion Items

BIS is adding new ECCNs 4A005 (equipment) and 4D004 (software), as well as an updated paragraph 4E001.a and a new paragraph.c (technology) to Category 4 of the CCL, where computing and processing items are regulated. These new controls cover equipment, software and technology used in cyber intrusion activities.

However, the new controls carve out the provision of basic software updates and upgrades, and activities relating to vulnerability disclosure and cyber incident responses. BIS also is amending 5A004 for systems, equipment and components for defeating, weakening or bypassing information security, to link to items in the new 4A005.

Surveillance Items

BIS is amending ECCN 5A001, which regulates sensitive telecommunications infrastructure, with a new paragraph 5A001.j covering internet IP network communications surveillance systems or equipment. Corresponding updates are being made to ECCNs 5B001 (test, inspection and production equipment), 5D001 (software) and 5E001 (technology) for items relating to the new 5A001.j.

Definitions

The terms "cyber incident response" and "vulnerability disclosure" are being added to the definitions section of the EAR at Part 772.

- Cyber incident response 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 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.

Exclusions from the New Controls

Published Information

Software and technology that are in the public domain and that meet the requirements to be considered "published" information under 15 C.F.R. § 734.7 will remain not subject to the EAR and, thus, are excluded from these controls.

Encryption Controlled Items

When a cybersecurity item also incorporates information security functionality such that it is subject to the encryption controls in Category 5, Part 2 of the EAR, those encryption controls will prevail, provided the information security functionality remains present and usable within the cybersecurity end item or executable software.

However, encryption controls do not take precedence for software source code or technology that implement functionality controlled elsewhere on the CCL, or for

any item where the information security functionality is absent, removed or otherwise non-existent.

Surreptitious Listening Controls

Items already controlled for surreptitious listening ("SL") s under another ECCN will continue to be classified under the relevant SL controlled ECCN.

New License Exception ACE

BIS is also establishing a new License Exception Authorized Cybersecurity Exports at Section 740.22 of the EAR. This is an evident response to the industry criticism in 2015, as BIS stated its intention behind ACE is to "avoid impeding legitimate cybersecurity research and incident response activities." The exception begins with definitions of the following terms, for specific use within the context of the ACE exception: "cybersecurity items," "digital artifacts," "favorable treatment cybersecurity end user" and "government end user."

Note that similar terms are used elsewhere with different meaning in the EAR. For example, License Exception GOV at Section 740.11 of the EAR for exports to government end users and License Exception ENC at Section 740.17 of the EAR for encryption exports both define the concept of a government end user differently. License Exception ACE takes a broader view of that term, covering traditional governmental functions, as well as government operated research institutions, entities and individuals who are acting on behalf of a government, and private sector entities such as retail or wholesale firms engaged in the manufacture, distribution or provision of defense articles or services.

As explained by BIS, License Exception ACE allows the export, reexport and transfer (in country) of cybersecurity items to most destinations, except to regions subject to trade embargoes. The exception also takes a restrictive approach to national security concern countries such as China and Russia.

In particular, ACE does not authorize exports for government end-users in Country Groups D:1, D:2, D:3, D:4 or D:5, as well as to nongovernment end-user in Country Group D:1 or D:5. However, BIS did include relief for certain exports to Country Group D countries that are also listed in the close ally Country Group A:6 – specifically Cyprus, Israel and Taiwan.

In addition, License Exception ACE will not permit end uses where the exporter has to know the cybersecurity item "will be used to affect the confidentiality, integrity or availability of information or information systems."

Survey of Comments Received

Although BIS asserted that it had appropriately tailored the new controls for narrow impact, it requested comments from industry to "ensure full consideration of the potential impact of this rule, including comments on the potential cost of complying . . . and any impacts this rule has on legitimate cybersecurity activities."

Thereafter, BIS published a dozen comments received from industry.

Most commenters shared the general theme that they viewed the rule as needing further tailoring.

There were requests for clarity around definitions of government end users, vulnerability disclosures and incident responses, as well as requests for more detailed guidance from BIS on implementation of the rule.

There may be further refinement of the rule yet to come.

Note

1. *https://www.govinfo.gov/content/pkg/FR-2021-10-21/pdf/2021-22952.pdf.*