SQUIRE PATTON BOGGS

US-EU-UK Export Controls and Sanctions Alert

December 2021

US Commerce Department Adopts Controls on Cyber Intrusion Item; Opportunity for Industry Comment

On October 21, 2021, the US Commerce Department's Bureau of Industry and Security (BIS) published in the Federal Register an Interim Final Rule with request for comments, that amends the Export Administration Regulations (EAR) (15 CFR Parts 730-774) regarding export controls on certain cyber intrusion items.

The new Interim Final Rule implements the Wassenaar Arrangement (WA) decisions from 2017 related to cybersecurity by: (1) adding the WA definitions for "cyber incident response," and "vulnerability disclosure" to part 772 of the EAR; (2) creating new and revising existing Export Control Classification Numbers (ECCNs) to control certain cyber intrusion items in Category 4 and Category 5 – Part 1 on the Commerce Control List (CCL); and (3) creating a new list-based License Exception Authorized Cybersecurity Exports (ACE) (new Part 740.22) and amending License Exception GOV (Part 740.11).

At a high level, the new Interim Final Rule establishes controls on the export, reexport or transfer (in-country) of certain items that can be used for cyber intrusion activities by adding and amending several ECCNs in Category 4 and Category 5 – Part 1 on the CCL. The cyber intrusion items controlled in Category 4 are controlled for national security reasons under NS column 1 and require a license for export, reexport or transfer to all countries except Canada. Category 5 – Part 1 is amended to control certain IP network communications surveillance items, which are controlled for national security reasons under NS column 2 and require a license for export, reexport or transfer to most countries.

Additionally, the rule creates a new License Exception ACE, which would authorize certain exports, deemed exports, reexports, deemed reexports or transfers (in-country) of certain "cybersecurity items" (as defined in License Exception ACE as the new ECCNs added and amended by this rule) to most countries, except: (1) to countries listed in Country Groups E:1 and E:2 (e.g., Cuba, Iran, North Korea and Syria) (Supp. No. 1 to Part 740); (2) to government end users of any country listed in Country Groups D:1, D:2, D:3, D:4, or D:5, except for certain items related to cybersecurity incidents destined to certain end users in a Country Group D country that also is listed in Country Group A:6; or (3) to non-government end users located in any country listed in Country Group D: 1 or D: 5.[1]

License Exception ACE also would not authorize exports, reexports or transfers where the party seeking to utilize License Exception ACE "knows" or had "reason to know" at the time of export, reexport or transfer (in-country), including deemed exports and reexports, that the cybersecurity item will be used for certain malicious cyber intrusion activities.

Effective Date: January 19, 2022.

Comments Due to BIS: December 6, 2021.

Definition of Terms

This Interim Final Rule adds the following WA definitions for "cyber incident response" and "vulnerability disclosure" to Section 772.1 of the EAR, both of which terms are used in the new and amended ECCNs and in the new License Exception ACE created by this Interim Final Rule.

- **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.

New and Amended ECCNS

The new Interim Final Rule adds several new ECCNs and amends several existing ECCNs as well, in order to describe the controls on the cyber intrusion items.

Category 4

This Interim Final Rule creates new ECCNs 4A005 and 4D004, as well as a new paragraph 4E001.c. Additionally, the Interim Final Rule applies the existing definition for "intrusion software" (Part 772.1) to these new ECCNs. The rule also revises 4D001.a to include 4A005.[2]

The new ECCNs 4A005 and 4D004, and the new paragraph 4E001.c control the following items:

- **4A005**: "Systems," "equipment," and "components" therefor, "specially designed" or modified for the generation, command and control, or delivery of "intrusion software."

1 This last restriction does not apply to (A) the export, reexport or transfer of certain cybersecurity items; (B) "vulnerability disclosure" or "cyber incident response" as those terms are defined in License Exception ACE; or (C) deemed exports.

2 In addition, to clarify the scope of existing entries in Category 5, Notes 3 and 4 are added to Category 4, which state as follows:

- **Note 3**: Commodities and "software" in ECCNs 4A005 and 4D005 that are also controlled in ECCNs 5A002.a, 5A004.b, 5D002.c.1, or 5D002.c.3, remain controlled in Category 5 – Part 2 by those entries. Category 5 – Part 2 does not apply to elements of source code that implement functionality controlled by these Category 4 ECCNs, or to any item subject to the EAR where Encryption Item (EI) functionality is absent, removed or otherwise non-existent.
- **Note 4**: Items in ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, and "technology" specified in ECCN 4E001 (for 4A005, 4D001.a (for 4A005 or 4D004) or 4D004) and 4E001.c that are also controlled for Surreptitious Listening (SL) reasons under another ECCN, will continue to be classified under the SL ECCN.

- **4D004**: "Software" "specially designed" or modified for the generation, command and control, or delivery of "intrusion software."[3]
- **4E001.c**: "Technology" for the "development" of "intrusion software."

"Intrusion software" is defined in part 772.1 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:[4]

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

Category 5 – Part 1

The Interim Final Rule adds a new paragraph 5A001.j, which controls the following telecommunications systems, equipment, "components" and "accessories":

j. IP network communications surveillance systems or equipment, and "specially designed" components therefor, having all of the following:

j.1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):

j.1.a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));

j.1.b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments)

j.2. Being "specially designed" to carry out all of the following:

j.2.a. Execution of searches on the basis of "hard selectors"

j.2.b. Mapping of the relational network of an individual or of a group of people.[5] [6]

Category 5 – Part 2

The new rule adds ECCN 4A005 to the existing paragraph 5A004.b, which now controls the following items:

b. Items not specified by ECCNs 4A005 or 5A004.a, designed to perform all of the following:

b.1. "Extract raw data" from a computing or communications device

b.2. Circumvent "authentication" or authorization controls of the device, in order to perform the function described in 5A004.b.1.

In addition to adding and amending the various ECCNs, the new Interim Final Rule provides two clarifications: (1) that items controlled because of encryption will remain in Category 5, Part 2; and (2) items previously controlled for Surreptitious Listening (SL) reasons under existing ECCNs will not be moved.[7]

3 **Note**: 4D004 does not apply to "software" specially designed and limited to provide "software" updates or upgrades meeting all of the following:

a. The update or upgrade operates only with the authorization of the owner or administrator of the system receiving it

b. After the update or upgrade, the "software" updated or upgraded is not any of the following:

1. "Software" specified by 4D004
2. "Intrusion software"

4 **Note** 1: "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: Network-capable devices include mobile devices and smart meters.

Technical note 1: "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: "Protective countermeasures": techniques designed to ensure the safe execution of code, such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) or sandboxing.

5 The new rule also adds the following exclusion note to 5A001.j:

Note: 5A001.j does not apply to "systems" or "equipment", "specially designed" for any of the following:

- Marketing purposes
- Network Quality of Service (QoS)
- Quality of Experience (QoE)

6 In addition, similar to the clarifying notes added in Category 4, the Interim Final Rule adds two clarifying notes to Category 5 – Part 1:

- **Note 3**: Commodities in ECCN 5A001.j, and related "software" specified in 5D001.c (for 5A001.j) that are also controlled in ECCNs 5A002.a, 5A004.a, 5A004.b, 5D002.c.1, or 5D002.c.3, remain controlled in Category 5 – Part 2 by those entries. Category 5 – Part 2 does not apply to elements of source code that implement functionality controlled by these Category 5 Part 1 ECCNs, or to any item subject to the EAR where Encryption Item (EI) functionality is absent, removed or otherwise non-existent.
- **Note 4**: Items in ECCN 56A001.j, 5B001.a (for 5A001.j), related "software" specified in 5D001.a (for 5A001.j) and 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)) and related "technology" specified in ECCN 5E001.a (for 5A001.j or 5D001.a (for 5A001.j)) that are also controlled for Surreptitious Listening (SL) reasons under another ECCN, will continue to be classified under the SL ECCN.

7 First, cybersecurity items that also incorporate particular "information security" functionality specified in certain Category 5 – Part 2 ECCNs (i.e., 5A002.a, 5A004.a, 5A004.b, 5D002.c.1, or 5D002.c.3) will be controlled under those Category 5 – Part 2 ECCNs, provided the controlled "information security" functionality remains present and usable within the cybersecurity end item or executable software.

Second, the new Interim Final Rule clarifies that all items subject to the EAR that are controlled for SL reasons under an existing ECCN that is not added to the CCL by this rule will continue to be classified under that existing SL ECCN. The WA changes related to "intrusion software" and IP network communications surveillance systems do not change any existing EAR provisions regarding communications intercepting devices, "software" or "technology," or any SL control (§ 742.13). Where an item is controlled for NS reasons because it meets multiple control parameters (i.e., cybersecurity parameters, encryption item (EI) parameters, and SL parameters), the most restrictive control will apply to the item.

License Exceptions

The new rule adds eligibility to the following ECCNs for License Exception ACE: 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)). The rule also revises the special conditions to make ECCNs 4D001.a and 4E001.a and .c ineligible to use License Exception STA, removes eligibility for License Exceptions STA, GBS, and LVS for ECCNs 5A001.j and 5B001.a, and removes eligibility for License Exceptions STA and TSR for 5D001.a and .c and for 5E001.a.

New License Exception ACE

The new Interim Final Rule creates a new License Exception ACE that authorizes exports, reexports and transfers (in-country) of "cybersecurity items", which are not also controlled in Category 5 – Part 2 of the CCL or for SL reasons. The new License Exception will be added in new § 740.22 of the EAR.

Scope of License Exception ACE

License Exception ACE authorizes exports, deemed exports, reexports, deemed reexports or transfers (in-country) of "cybersecurity items" (defined below) to most destinations, except: (1) to nationals of countries listed in in country groups E:1 or E:2 in Supplement No. 1 to Part 740 of the EAR;[8] (2) certain "government end-users";[9] and (3) subject to certain end-use restrictions.[10]

Definitions

Section 740.22(b) provides the following definitions for "cybersecurity items," "digital artifacts," "favorable treatment cybersecurity end user," and "government end user," as those terms are used in License Exception ACE:

- Cybersecurity Items are 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)).
- Digital artifacts are items (e.g., "software" or "technology") found or discovered on an information system that show past or present activity pertaining to the use or compromise of, or other effects on, that information system.
- Favorable treatment cybersecurity end user is any of the following:
  - A "U.S. subsidiary"
  - Providers of banking and other financial services
  - Insurance companies
  - Civil health and medical institutions providing medical treatment or otherwise conducting the practice of medicine, including medical research
- Government end user, for purposes of § 740.22, is 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.

Restrictions

Section 740.22(c) of License Exception ACE provides the following restrictions on the export, deemed export, reexport, deemed reexport, or transfer (in-country) of "cybersecurity items":

- **Destination or end-user restrictions**. License Exception ACE does not authorize deemed exports under paragraph (c)(1)(i) or (ii) of this section. The restrictions in paragraphs (c)(1)(i) and (ii) apply to activities, including exports, reexports, and transfers (in-country) related to "vulnerability disclosure" and "cyber incident response." However, Note 1 to ECCN 4E001 in the CCL (supplement No. 1 to part 774 of the EAR) excludes "vulnerability disclosure" and "cyber incident response" from control under 4E001.a or .c.
  - A destination that is listed in Country Group E:1 or E:2 in supplement no. 1 to part 740 of the EAR.
  - A government end user, as defined in this section, of any country listed in Country Group D:1, D:2, D:3, D:4, or D:5 in supplement no. 1 to part 740. This restriction does not apply to:
    - Exports, reexports and transfers (in-country) to Country Group D countries that are also listed in Country Group A:6 of "digital artifacts" that are related to a cybersecurity incident involving information systems owned or operated by a "favorable treatment cybersecurity end user", or to police or judicial bodies in Country Group D countries that are also listed in Country Group A:6 for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents.
    - Exports, reexports, and transfers (in-country) to national computer security incident response teams in Country Group D countries that are also listed in Country Group A:6 of "cybersecurity items" for purposes of responding to cybersecurity incidents, for purposes of "vulnerability disclosure", or for purposes of criminal or civil investigations or prosecutions of such cybersecurity incidents.
  - A non-government end user located in any country listed in Country Group D:1 or D: 5 of Supplement No. 1 to part 740 of the EAR. This restriction does not apply to:
    - Exports, reexports or transfers (in-country) of cybersecurity items classified under ECCNs 4A005, 4D001.a (for 4A005 or 4D004), 4D004, 4E001.a (for 4A005, 4D001.a (for 4A005 or 4D004) or 4D004) and 4E001.c, to any "favorable treatment cybersecurity end user."
    - "Vulnerability disclosure" or "cyber incident response."
    - Deemed exports.
- **End-use restrictions**. License Exception ACE is not authorized if the exporter, reexporter, or transferor "knows" or has "reason to know" at the time of export, reexport or transfer (in-country), including deemed exports and reexports, 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).

8 Described in paragraph (c)(1)(i) of License Exception ACE

9 Described in (c)(1)(ii) of License Exception ACE

10 Described in (c)(2) of License Exception ACE

Amended License Exception GOV

In addition to creating new License Exception ACE, the Interim Final Rule amends License Exception Governments, international organizations, international inspections under the Chemical Weapons Convention, and the International Space Station (GOV) in § 740.11, to exclude "cybersecurity items"[11] as defined in License Exception ACE from paragraph (c) of License Exception GOV.

Amended License Exceptions STA, GBS, LVS and TSR

Finally, the new Interim Final Rule also revises several other License Exceptions. Specifically, License Exception STA is revised as follows for the following ECCNs when the destination is listed in Country Groups A: 5 or A: 6:

- The special conditions for License Exception STA are revised to include the ineligibility of:
  - Software specified in 4D001.a "specially designed" for the "development" or "production" of equipment specified by ECCN 4A005 to Country Groups A: 5 and A: 6
  - Technology controlled under 4E001.a (for 4A005 and 4D004)
  - Technology controlled under 4E001.c
- To remove eligibility for:
  - 5A001.j
  - 5B001.a (for items "specially designed" for the "development" or "production" of 5A001.j)
  - 5D001.a (for equipment, functions or features specified by 5A001.j)
  - 5D001.c (for equipment specified by 5A001.j or 5B001.a)
  - 5E001.a (for 5A001.j, 5B001.a (for 5A001.j), 5D001.a (for 5A001.j), or 5D001.c (for 5A001.j or 5B001.a (for 5A001.j))

Additionally, License Exceptions GBS and LVS also are revised to remove eligibility for items classified under 5A001.j and 5B001.a (for 5A001.j). License Exception TSR is revised to remove eligibility for software classified under 5D001.a (for 5A001.j) or 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)) and for technology classified under 5E001.a for 5A001.j, 5B001.a (for 5A001.j), 5D001.a (for 5A001.j), or 5D001.c (for 5A001.j or 5B001.a (for 5A001.j)).

Contacts

Please feel free to contact one of the trade practitioners listed or you can reach our team collectively via email.

US

George N. Grammas
Partner, Washington DC/London
T +1 202 626 6234
T +44 20 7655 1301
E george.grammas@squirepb.com

Daniel E. Waltz
Partner, Washington DC
T +1 202 457 5651
E daniel.waltz@squirepb.com

Karen R. Harbaugh
Partner, Washington DC
T +1 202 457 6485
E karen.harbaugh@squirepb.com

EU

Robert MacLean
Partner, Brussels
T +32 2 627 7619
E robert.maclean@squirepb.com

José María Viñals
Partner, Madrid/Brussels
T +34 91 426 4840
T +32 2 627 1111
E josemaria.vinals@squirepb.com

UK

Matthew Kirk
International Affairs Advisor, London
T +44 20 7655 1389
E matthew.kirk@squirepb.com

International Trade Practice co-leaders: Frank Samolis (partner, Washington DC) and George Grammas

About Us

Our export controls and sanctions lawyers have the ability to provide advice on the shifting regulatory framework on both sides of the Atlantic. We have extensive experience in advising and representing a wide range of companies and financial institutions in Europe, the US and other jurisdictions on export control and sanctions from a multijurisdictional perspective. Our team is part of our overall International Trade Practice, providing a "one-stop shop" solution to global trade compliance through rapid, professional and tailored advice and compliance tools to fit your business needs and processes.

ITAR Handbook

Organizations engaged in the trade of items specially designed for military or space applications are encouraged to download our complimentary *ITAR Practitioner's Handbook*, which covers the International Traffic in Arms Regulations (ITAR) and the US Department of Commerce "600 Series."

11 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))