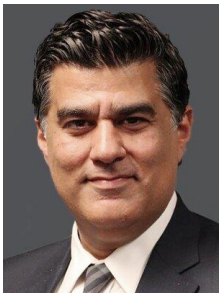
Applying Commerce Dept.'s New Cybersecurity Export Rule

By **Tamer Soliman, Rajesh De and Anjani Nadadur** (August 23, 2022)



Tamer Soliman

Rajesh De

Anjani Nadadur

The U.S. government continues to enhance its export controls on cybersecurity items.

On May 26, the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, published a final rule revising the restrictions on the export, reexport and transfer in-country of certain cybersecurity items used for malicious cyberactivities.

Effective immediately upon publication, the final rule amends the Oct. 21, 2021 interim final rule that went into effect March 7. More specifically, the final rule:

- Added a new end-use restriction[1] to license exception for encryption commodities, software and technology, or ENC, in order to mirror the end use restrictions applicable to the existing license exception for authorized cybersecurity exports, or ACE, and close a potential loophole for certain items;
- Limited the scope of carveouts available under License Exception ACE for certain government end users to only account for digital artifacts used in connection with criminal or civil investigations or with prosecutions of cybersecurity incidents;
- Further defined government end user under License Exception ACE by providing an illustrative list of seven types of users who meet the definition and added a definition for "partially operated or owned by a government or governmental authority"; and
- Made a number of structural clarifications and restored 5D001.e, which was inadvertently removed from the interim rule, to Export Control Classification Number 5D001.

The final rule also included structural changes and clarifications in response to public comments.

Background

The final rule was preceded by an interim rule, which was published on Oct. 20, 2021, and went into effect March 7.

The interim rule implemented long-anticipated and debated export controls on intrusion software[2] that balanced U.S. foreign policy and national security concerns with the need for maintaining a regulatory framework that allows for legitimate cybersecurity transactions.

The language of the interim rule reflected several years of negotiations codified in the multilateral 1996 Wassenaar Arrangement and incorporated significant U.S. stakeholder input received by BIS over the years through its various attempts to propose the controls.

Export Controls on Cybersecurity Items

The final rule clarifies the licensing requirements and applicability of license exceptions relating to the export of certain cybersecurity items that can be used for malicious cybersecurity activities — whether goods, software or technology — to most destinations except Canada. This includes:

- Software, hardware and technology specially designed to generate, command and control or deliver intrusion software; and

- Certain IP network communications surveillance tools.

In the case of items controlled under the International Traffic in Arms Regulations, the U.S. export controls regime governing defense items and services, items incorporating particular information security encryption functionality specified under Category 5 — specifically, 5A002.a, 5A004 a-b, 5D002.c.1 or 5D002.c.3 — and items controlled under the Export Administration Regulations, or EAR, for surreptitious listening or national security reasons are still controlled under those standards.

License Exception ACE

License Exception ACE, which was established by the interim rule, authorizes the export of most U.S.-origin cybersecurity items to most destinations.

While not available at all for certain countries — Cuba, Iran, North Korea and Syria — for nearly 40 other countries, including China, License Exception ACE contains a complex series of limitations and conditions extending to both government end users in Country Group D, as listed in Title 15 of the Code of Federal Regulations, Part 740, Supplement No. 1, and nongovernment end users located in countries listed in Country Groups D:1 or D:5 for U.S. national security or arms embargo concerns, including Sudan, Syria, Venezuela and Vietnam.

The recently published final rule added an illustrative list of end users that meet the definition of a government end user under License Exception ACE, differentiating between more sensitive government end users and less sensitive government end users, which are terms already defined in the EAR.[3]

The final rule also amended these definitions in the EAR to clarify that they apply to cybersecurity items and are now referenced in License Exception ACE.[4]

In the final rule, BIS also included the expression "partially operated or owned by a government or governmental authority" in three categories of listed government end users — utilities, transportation hubs and services, and retail or wholesale firms — and added a note to define the expression.[5]

Parties involved in transactions involving the export of controlled cybersecurity items must ensure that the contemplated activity is consistent with these limitations when seeking to avail themselves of License Exception ACE.

What Exceptions Apply to Government End Users?

License Exception ACE allows for two limited carveouts to allow exports to government end users in countries simultaneously listed in Country Group D and A:6 — currently, Cyprus, Israel and Taiwan — that might not otherwise qualify for the license exception, including the following:

- Exports of digital artifacts — i.e., software or technology found or discovered on an information system that show activity pertaining to the use or compromise of, or other effects on, that system — on information systems owned or operated by a favorable treatment cybersecurity end user, such as U.S. subsidiaries, banking institutions, insurance companies or civil health and medical institutions, or to police or judicial bodies in these countries for purposes of criminal or civil investigations or prosecutions.

- Exports to national computer security incident response teams for purposes of responding to cybersecurity incidents, engaging in vulnerability disclosures for remediation purposes or to assist police or judicial bodies in these countries for the purposes of cybersecurity investigations or prosecutions.

Furthermore, License Exception ACE broadly affords favorable treatment for vulnerability disclosures and cyber incident response, with respect to nongovernment end users through an exclusion. For Group D government end users, License Exception ACE does not contain a similar general exclusion for these activities.

However, there is a limited exclusion for such activities from the scope of control under one technology classification 4E001.c technology for the development of intrusion software. Because that exclusion is at the controlled item level, rather than the License Exception ACE level, it does not depend on whether the end user is a government or nongovernment end user.

To the extent the only technology to be transferred in the course of vulnerability disclosure and cyber incident response[6] would otherwise be controlled as technology for the development of intrusion software, the note to 4E001.c provides limited relief. This carveout does not otherwise exempt or exclude such activities more generally.

Apart from these limited carveouts, License Exception ACE is not available for government end users in Country Group D. Moreover, in both cases, the availability of License Exception ACE is subject to the other conditions and requirements of the EAR, including that there be no reason to know of a malicious cyber end-use under the end-use restriction described below.

In addition to the end-user restrictions, License Exception ACE does not apply where there is either knowledge or

> reason to know at the time of export, reexport, or transfer (in-country) ... that the "cybersecurity item" will be used to affect the confidentiality, integrity, or availability of information or information systems, without the authorization by the owner, operator, or administrator of the information system.

It is important to note that BIS interprets "knowledge" or "reason to know" broadly in a manner that does not require a showing of positive knowledge or awareness of the

existence of a fact and regularly evaluates whether there was knowledge or reason to know based on the facts and circumstances surrounding the transaction.

Any party relying on License Exception ACE should carefully consider and apply appropriate risk-based due diligence to evaluate potential prohibited end-user and end-use considerations in order to mitigate potential exposure in connection with these controls.

What Limitations Apply for Nongovernment End Users?

License Exception ACE imposes restrictions for nongovernmental end users, users that do not fall into the definition of government end user, in countries in Country Groups D:1 or D:5 but not countries in Groups D:2, D:3 or D:4.[7] For nongovernment end users in these countries, License Exception ACE is not available, subject to certain limited carveouts for:

- Certain cybersecurity items to favorable treatment cybersecurity end users;
    - Controlled cybersecurity items covered by the 4A005, 4D001.a, 4D004, 4E001.a and 4E001.c export control classifications to favorable treatment cybersecurity end users who are not government end users remain eligible for ACE;
    - Exports of cybersecurity items covered by other export control classifications are outside the scope of this carveout, even if the end user is a favorable treatment cybersecurity end user;
- Cybersecurity items — goods, software and technology — provided for vulnerability disclosure and cyber incident response;
    - Nongovernment end users in Group D:1 or D:5 does not apply to vulnerability disclosure and cyber incident response.

Apart from these limited carveouts, License Exception ACE is not available for nongovernment end users in Country Groups D:1 or D:5.

Moreover, in both cases, the availability of License Exception ACE is subject to the other conditions and requirements of the EAR, including that there be no reason to know of a malicious cyber end use under the end-use restriction, as described above.

New End Use Restriction for License Exception ENC

In the final rule, BIS added a new end-use restriction to Title 15 of the Code of Federal Regulations, Section 740.17, to prohibit the use of License Exception ENC for certain cybersecurity items[8] if there is either knowledge or

> "reason to know" at the time of export, reexport, or transfer (in-country) ... that the 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.

This language, which adds cryptographic or cryptanalytic functionality to the cybersecurity item, mirrors that of License Exception ACE and is intended to close a loophole and prevent the evasion of ACE restrictions by use of ENC.

Conclusion

Any party relying on License Exceptions ENC or ACE should carefully consider and apply appropriate risk-based due diligence to evaluate potential prohibited end-user and end-use considerations in order to mitigate potential exposure in connection with these controls.

Specifically, practitioners should consider the following:

- Whether items that are being exported outside the U.S. could be controlled as cybersecurity items;
- Whether other standards apply, e.g., ITAR, certain encryption controls, or surreptitious listening or national security controls;
- The country of destination for these items and its eligibility under License Exception ACE;
- The proposed end user of these items and whether they would fall within one of the categories of government end users; and
- The proposed end use or purpose for these items, including whether any exception would apply.

Tamer Soliman is a partner and global head of the export control and sanctions practice at Mayer Brown LLP.

Rajesh De is a partner and head of the firm's global cybersecurity and data privacy, and national security, practices.

Anjani Nadadur is an associate at the firm.

Mayer Brown associates Gretel Echarte and Ellen Aldin also contributed to this article.

[1] 15 C.F.R. § 740.17(f).

[2] '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: (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." § 772.

[3] See 15 C.F.R. § 772 for a complete list of terms defined in the EAR.

[4] 15 C.F.R. § 740.22(b)(4).

[5] 15 C.F.R. § 740.22(b)(5).

[6] "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."

[7] Non-government end-users in Group D countries not falling under D:1 or D:5, such as Bahrain, Israel, Jordan, Oman, Pakistan, Qatar, Saudi Arabia and the UAE, are not covered by the non-government end-user restrictions on License Exception ACE.

[8] These items include:

- "cryptanalytic items," classified in ECCN 5A004.a, 5D002.a.3.a or c.3.a, or 5E002;
- network penetration tools described in § 740.17(b)(2)(i)(F), and ECCN 5E002 "technology"; or
- automated network vulnerability analysis and response tools described in § 740.17(b)(3)(iii)(A), and ECCN 5E002 "technology."