On June 3, 2016, the U.S. Department of Commerce’s Bureau of Industry and Security (BIS) and U.S. Department of State’s Directorate of Defense Trade Controls (DDTC) published final rules revising fundamental definitions in the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR), respectively. These revisions make substantive changes to the operation of the EAR and ITAR, notably to decontrol certain encrypted transfers of software and technology. BIS has also published FAQs related to these revisions. The revisions are part of the ongoing export control reform efforts of BIS and DDTC and are designed to enhance clarity and consistency between the two sets of regulations in both design and effect.

The definitions of “export,” “reexport,” “release,” and “retransfer” were revised in both the EAR and ITAR, with the definitions of “access information,” “technology,” “required,” “foreign person,” “proscribed person,” “published,” results of “fundamental research,” “transfer,” and “transfer (in-country)” also being revised in the EAR. The revisions are largely in line with the proposed rules published on June 3, 2015 (on which we reported previously), and the main changes from the proposed rules are discussed below. The final rules are effective September 1, 2016. DDTC’s final rule only covers some of the definitions included in its proposed rule, while the remainder will be the subject of future rulemakings.

Effect of Encryption on Exports: Authorization for Cloud Computing

The most consequential change in the final rule published by BIS is the definition of “activities that are not exports, reexports, or transfers” to decontrol certain sending, taking, or storing of encrypted technology or software.

The final rule applies a four-part test in order to determine if the sending, taking, or storing technology or software will not be considered a controlled export transaction:

- The technology or software must be unclassified;
- “End-to-end encryption” must be used to secure the technology or software;
- The encryption technology in use must meet or exceed Federal Information Processing Standards (FIPS) Publication 140-2 and be supplemented by security-related software meeting or exceeding current NIST guidance; and
- The technology or software must not intentionally be stored in a country listed in Country Group D:5 or in Russia.
“End-to-end” encryption is defined as data that is not in an unencrypted form between the originator and the intended recipient, and the means of decryption have not been provided to a third party. The proposed rule imposed a requirement that the data not be decrypted at any point between the initiation of the transmission and its receipt. BIS relaxed this requirement in the final rule, rewording the definition to allow for decryption and re-encryption during the course of transmission for technical reasons (such as to establish a VPN connection or to transmit data among servers), so long as any decryption and re-encryption are within the in-country security boundary of either the originator or recipient, and no third party has the ability to access the unencrypted data.

The final rule includes a corresponding section which states that the provision of “access information,” such as decryption keys, passwords, or other information that would allow access to encrypted data that was sent, taken, or stored under this provision, is subject to the same export control requirements that would apply to the data if the data were not encrypted. BIS clarified that a victim of a database hack or other breach in security related to encrypted data covered under this section of the EAR would not be considered responsible for the export, reexport, or transfer of that data, so long as the originator of the technology did not provision access information or otherwise allow the unauthorized person to gain access to the encrypted data.

This final rule will allow U.S.-based companies to use cloud technology and other electronic transmission systems (including email) to transfer and store unclassified technology and software subject to the EAR without facing export control requirements, so long as they meet the encryption requirements specified in the rule. BIS has also clarified in its FAQs that this section of the final rule allows for secure remote access to data on a U.S. server by a U.S. national while outside the United States without it being considered an export under the EAR.

Notably, the proposed rule by DDTC published in 2015 contained a similar provision allowing for the sending, taking, or storing of encrypted technology or software controlled by the ITAR. This provision will be included in a separate rulemaking in the future, so this cloud computing authorization is not currently in effect under the ITAR.

**Transfers of Certain Information Between U.S. Persons Overseas Not an Export**

Both the EAR and ITAR have been revised to adopt language decontrolling transfers of certain information between or among U.S. persons located outside the United States. The contours of the authorizations are different, so careful attention must be paid to what is permitted for a given transfer and which set of regulations applies.

The EAR added a provision to its definition of “activities that are not exports, reexports, or transfers” to authorize the transfer of technology or software between or among U.S. persons who are located in the same foreign country. Such a transfer remains exempt from the definition of export, reexport, or transfer, so long as the transmission or transfer does not result in a release to a foreign person or to a person prohibited from receiving the technology or software.

The ITAR added an additional exemption of general applicability from its licensing requirements when technical data (including classified information) is exported, reexported, or retransferred by or to a U.S. person or a foreign person employee of a U.S. person travelling or on temporary assignment abroad. The exemption includes several restrictions. Like the provision added to the EAR, the technical data must be secured against release to an unauthorized person. Transfers to or from foreign person employees under this exemption must relate to persons who are authorized to receive ITAR-controlled technical data under a separate license or approval. Similarly, the individual sending or receiving ITAR-
controlled data must be an employee of the U.S. government or be directly employed by a U.S. person and not by a foreign subsidiary. Technical data authorized under this exemption is not permitted to be used for foreign production purposes or defense services without a license or separate approval. Though the exemption applies to classified information, any transfer of classified information outside the United States must be conducted in accordance with Department of Defense requirements.

**Release of Technology to a Foreign Person Clarified**

The revisions to the EAR include a change to the definition of “release.” Previously, the EAR stated that a visual inspection of technology or source code by a foreign person was sufficient by itself to constitute a release of that technology or source code to a foreign person (and thus a deemed export to the home country of that foreign person). The revised definition of release heightens the standard for a release, requiring a “visual or other inspection” of an item that actually reveals technology or source code to the foreign person. BIS stated that merely seeing an item is not necessarily sufficient to constitute a release of the technology required to develop or produce it. Similarly, merely providing foreign persons with access to controlled equipment, software, or technology in the United States does not necessarily constitute a release. On the other hand, oral or written exchanges with a foreign person of technology or source code would constitute a release. The ITAR added a definition of “release” with the same terms in order to harmonize its definitions with the EAR.

**Codification of Different Deemed Export Policies Under the EAR and ITAR**

The final rule published by BIS retains the “deemed export” rule set forth in EAR § 734.2(b). A release of technology or source code subject to the EAR to a foreign national, including within the United States, is deemed to be an export to the home country or countries of that foreign national. The final rule codifies the long-standing BIS policy that such an export is deemed to occur to that person’s most recent country of citizenship or permanent residency.

The ITAR contains a similar rule in § 120.17(4), holding that disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, is an “export” for purposes of the ITAR. The final rule published by DDTC does not adopt the BIS policy that a deemed export is only deemed to occur to the foreign national’s most recent country of citizenship or permanent residency, but rather was revised to state that such an export is deemed to be an export to all countries in which the foreign national holds or has held citizenship or holds permanent residency.

This difference typifies the policy differences between the ITAR and the EAR in the export control reform process. DDTC notes that a key tenet of export control reform is that the ITAR “will have higher walls around fewer, more sensitive items.” Accordingly, the more stringent deemed export rule is maintained as an example that the ITAR imposes stricter controls due to the more sensitive nature of the items controlled by it.

Similarly, BIS clarified that sending an item to the United States is not a “reexport” for purposes of the EAR. BIS noted that the EAR has no provisions controlling or otherwise pertaining to the act of importing items into the United States. This is in contrast to the ITAR, which contains extensive provisions regulating the import of defense articles into the United States.

**Key Takeaways**

The final rules affect fundamental definitions of the EAR and ITAR, and, accordingly, may affect a wide variety of businesses that export items controlled on the CCL or USML. The most notable change is the
authorization for cloud computing and other electronic transfers of encrypted technology or software subject to the EAR. This change signifies a recognition by BIS that encrypted information should not be subject to onerous export control authorization requirements if it is unable to be accessed. Please note, however, that since the corresponding rule is not yet in effect under the ITAR, U.S. companies may be limited in their use of cloud computing with respect to ITAR-controlled technical data.

These rules also allow for U.S. persons located abroad to, in certain situations, transfer information controlled by the EAR or ITAR between or among themselves without the transfer being subject to the licensing requirements of the EAR or ITAR. Exporters should be careful to note that the proposed rules and final rules are different and signify a divergence between the EAR and ITAR in certain ways. For example, the transfer of encrypted technology controlled under the ITAR remains subject to ITAR licensing requirements until DDTC publishes a follow-up rule. Similarly, the EAR and ITAR authorizations for transfers between certain persons while outside of the United States operate differently and have different requirements.

If you have any questions regarding the revisions to the EAR or ITAR or how they may affect your business, please reach out to the contacts listed below.

** * * * *

**Authors:**

Michael T. Gershberg

Justin A. Schenck
This alert is not intended to provide legal advice, and no legal or business decision should be based on its content. If you have any questions about the contents of this alert, please call your regular Fried Frank contact or the attorneys listed below:

**Contacts:**

**Washington, D.C.**

Michael T. Gershberg  
+1.202.639.7085  
michael.gershberg@friedfrank.com

**London**

Dr. Tobias Caspary  
+44.20.7972.9618  
tobias.caspary@friedfrank.com

Fried Frank’s [International Trade and Investment Group](#) regularly represents clients in international mergers and acquisitions, joint ventures, principal investments, and sensitive corporate investigations, particularly in relation to matters that implicate the U.S. government's regulation of international business activities, such as the Committee on Foreign Investment in the United States (CFIUS), economic sanctions, export controls, and anti-corruption and anti-bribery.

For decades, our international trade and investment practitioners have been consistently recognized for their legal and policy-based contributions. Today, our practice is unique among its kind: it draws upon the Firm’s long tradition of senior U.S. government and diplomatic service, combines policy insight with deep technical expertise and business judgment, is fully integrated with Fried Frank’s preeminent Corporate and Litigation Practices, and is international in its outlook, experience, network reach and reputation.