BIS and DDTC Issue Proposed Rules to Revise Key Definitions, Decontrol Certain Transfers of Encrypted Information

On June 3, 2015, 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 proposed rules revising key definitions in the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR) to harmonize the two export control regimes. The proposed rules would make certain substantive changes, most notably excluding from the definition of “export” the transfer and storage of technology or software in encrypted form, subject to certain conditions. For the most part, the revisions are intended to harmonize the substance and structure of the EAR and ITAR as part of the ongoing export control reform process, as well as to codify existing policies.

The proposed rules would revise important EAR and ITAR definitions, including the following: “export,” “reexport,” “technology” and “technical data,” “release,” “transfer,” “required” and “peculiarly responsible,” “published” and “public domain,” and “defense services.” While certain differences will remain between the two legal regimes, these proposed rules seek to make the language and structure of the EAR and ITAR more consistent. The Administration’s intent is to facilitate export compliance by harmonizing the two legal regimes, thus furthering the policy goals of the export control rules, and to take another step toward the ultimate export control reform objective of creating a common set of regulations. Most of the proposed revisions would not substantively change the existing rules. Instead, they would foster substantive harmonization (i.e., using the same words for the same concepts in the EAR and ITAR) and structural harmonization (i.e., using similar definitions in a common format that makes the differences clear).

The agencies have both published on their websites a chart showing a side-by-side comparison of the two sets of proposed regulatory language. BIS and DDTC will accept public comments on the proposed rules until August 3, 2015. We summarize below the main provisions of the proposed rules and their potential effect on exporters of U.S.-controlled items.

Export of Encrypted Information

The main substantive aspect of the proposed rules is to decontrol the transfer and storage of technology and software encrypted according to certain requirements. This change reflects recent developments in
the way data is shared and stored (e.g., cloud computing), and responds to suggestions that industry has made for years. It is the first recognition by BIS and DDTC that properly encrypted information does not pose a national security risk because it cannot be accessed. In particular, the rules would state that the terms export, reexport, release, retransfer, and transfer would exclude sending, taking, or storing technology/technical data or software that is (1) unclassified, and (2) secured using end-to-end encryption. These rules would include the following conditions and notes:

- The information must be secured using cryptography compliant with FIPS 140-2, supplemented by procedures and controls in accordance with NIST publications and guidance. BIS would also allow “similarly effective cryptographic means,” while DDTC would strictly require FIPS 140-2-compliant cryptography.

- EAR-controlled information could not be stored in a country listed in Country Group D:5 or Russia. ITAR-controlled technical data could not be stored in any country proscribed under ITAR Section 126.1 or Russia.

- “End-to-end encryption” requires “uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself.” Therefore, qualifying cloud providers may not store the data unencrypted, or decrypt/re-encrypt the data anytime before delivery to the intended recipient.

- The ability to access encrypted technology/technical data or software would not be considered a release or reexport of such items.

Under these proposed rules, U.S. companies would be able to transfer and store their unclassified export-controlled data using cloud computing and email systems without any export control obligations (subject to the encryption requirements). Currently, industry is reluctant to use such solutions for controlled data, despite their cost and efficiency benefits, because cloud system providers often rely on servers around the world and even foreign national employees in the United States. Under current rules, these patterns could constitute exports or deemed exports that require licenses or other authorizations. While this proposed change could provide a great benefit to many companies, it would also create a compliance risk because of the strict encryption requirements.

Export and Reexport

BIS and DDTC propose restructuring the definitions of “export” and “reexport,” which would generally mirror each other. One substantive change to these definitions is to add that an export includes the release or other transfer of the means of access to encrypted data. Since the transfer of properly encrypted data would not constitute an export, providing the decryption key, password, or other means of accessing the data must result in the return of export control requirements for the technology/technical data or software. However, BIS (but not DDTC) would only consider this transfer to result in an export if the release or transfer occurred with knowledge that it would cause or permit the transfer of technology/technical data in clear text to a foreign national. This is one of the few areas of difference between the two proposed rules.

The proposed rules would also codify current agency practice regarding the interpretation of nationality under the EAR and ITAR. The BIS rule states that a deemed export to a foreign national is considered an export “to the foreign national’s most recent country of citizenship or permanent residency.” Yet, the DDTC rule states that a deemed export to a foreign national is considered an export “to all countries in which the foreign national has held citizenship or permanent residency.”
In the related definition of “release,” one notable change is that a visual inspection by foreign nationals would only be considered a controlled release if it actually reveals technology/technical data or software source code to that foreign national. This definition also codifies another existing BIS agency practice (similar to the ITAR concept of a defense service) that a release of technology or source code includes the application abroad of personal knowledge or technical experience acquired in the United States, to the extent that such application actually reveals technology or software source code to a foreign national. Finally, the BIS rule would codify its current guidance on deemed reexports, which treats these transfers consistently with the license exemptions in ITAR Sections 124.16 and 126.18.

Technology and Technical Data

While the definitions of “technical” and “technical data” would be revised in several largely non-substantive ways, one notable aspect is the codification of BIS’ existing practice that “use” technology must meet all six activities in the definition (operation, installation (including on-side installation), maintenance (checking), repair, overhaul, and refurbishing). The definitions would now also include decryption keys or other means that would allow access to encrypted technology/technical data in clear text.

In determining which information is considered controlled technology/technical data, the proposed rules have clarified the term “required.” They also add new definitions for the currently undefined term “peculiarly responsible,” which largely mirrors the catch-and-release aspects of the “specially designed” definition.

Items Subject to the EAR and ITAR

The proposed rules would largely align the EAR provision for items subject to the EAR and the ITAR definition of defense articles. They would clarify when technology or software is published (under the EAR) or in the public domain (under the ITAR), two analogous concepts. They would also streamline the provisions on patents and fundamental research, without making any substantive changes. However, the EAR and ITAR definitions of fundamental research would still differ somewhat.

Conclusion

These proposed rules may affect a wide range of exporters. While many of the changes are merely structural or semantic, there are several substantive changes that may determine when items and transactions are subject to U.S. export control rules. Even the non-substantive changes may aid exporters in ensuring compliance by harmonizing the two separate export control regimes and making key definitions more consistent. BIS and DDTC will accept comments on the proposed rules until August 3, 2015. One interesting note is that the proposed rules would become effective 30 days after the final rules are published – rather than the usual six-month grace period for export control reform rules – because these rules do not actually change the CCL and USML control lists. Accordingly, once final rules are issued, exporters will have a relatively short time to incorporate these changes into their compliance policies and procedures.

If you have any questions regarding the proposed rule or would like to file comments with BIS or DDTC, please reach out to the contacts listed below.

* * *
Authors:

Hon. Mario Mancuso
Michael Gershberg

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:

Hon. Mario Mancuso  +1.202.639.7055  mario.mancuso@friedfrank.com
Michael Gershberg  +1.202.639.7085  michael.gershberg@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.