BCR

BERLINER CORCORAN & ROWE LLP

January 8, 2020

Regulatory Alert: DDTC Issues Changes to Definitions, Clarifying Impact of Encryption for Cloud Computing and Other Purposes

Export Controls and Sanctions Group

Benjamin H. Flowe, Jr.

John A. Ordway

Daniel Fisher-Owens

Babak Hoghooghi

Perry S. Bechky

Ray Gold

Jason A. McClurg

Michelle Turner Roberts

For more information on this Alert, please contact Dan Fisher-Owens (dfo@bcr-dc.com), John Ordway (jao@bcr-dc.com), or Jason McClurg (jam@bcr-dc.com), or your regular contact at BCR.

To subscribe to our practice group Alerts, please contact exportalerts@bcr-dc.com.

After several years of consideration, the State Department's Directorate of Defense Trade Controls ("DDTC") issued an Interim Final Rule on December 26, 2019 (84 Fed. Reg. 70887) adding a definition to the International Traffic in Arms Regulations ("ITAR") to parallel similar 2016 changes to the Commerce Department's Export Administration Regulations ("EAR"). The ITAR changes are effective March 25, 2020, with public comments to be submitted by January 27, 2020.

New ITAR § 120.54 provides that certain activities do not constitute an "export," "reexport," "retransfer," or "temporary import," and are thus not subject to ITAR authorization requirements.

Tracking EAR § 734.18(a)(1)-(4), new ITAR § 120.54(a)(1)-(4) will confirm that the ITAR does not regulate launching an item into space, transfers between U.S. persons within the United States, transfers between U.S. persons within the same foreign country, or transfers between the United States and its outlying possessions (e.g., Puerto Rico), so long as the transmission or transfer does not result in a release to a foreign person or to a person prohibited from receiving defense articles, technical data, or defense services (*e.g.*, a debarred person).

The most significant change is the adoption of an encryption standard in ITAR § 120.54(a)(5), paralleling EAR § 734.18(a)(5). When the rule becomes effective, the ITAR will not regulate sending, taking, or storing technical data that is:

(i) Unclassified;
(ii) Secured using end-to-end encryption;
(iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES–128);
(iv) Not intentionally sent to a person in or stored in a country proscribed in ITAR § 126.1 or the Russian Federation; and
(v) Not sent from a country proscribed in ITAR § 126.1 or the Russian Federation.

DDTC defines "end-to-end encryption" in new §120.54(b)(1) as: "(i) The provision of cryptographic protection of data, such that the data is not in an unencrypted form, between an originator (or the originator's in-country security boundary) and an intended recipient (or the recipient's in-country security boundary); and (ii) The means of decryption are not provided to any third party." The originator and the intended recipient may be the same person. The intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, such as by a license or other approval pursuant to the ITAR.

These changes began as part of the Obama Administration's Export Control Reform initiative, to establish clearer rules concerning use of cloud storage for export-controlled items. DDTC delayed implementation due to concerns about tracking the EAR's language that allows the data be secured using either FIPS 140-2 certified encryption means or by "equivalent" encryption. DDTC's rule allows use of either FIPS 140-2 certified encryption means, or encryption that provides "security strength that is at least comparable to" the AES 128-bit symmetric encryption algorithm, which is the FIPS 140-2 minimum standard. So, the ITAR requirement is stated differently, but is effectively the same as the EAR's requirement.

Otherwise, the EAR and ITAR provisions are substantially identical, with variations to address ITAR jurisdiction over temporary imports, and to conform to differences in regulatory terms. While these changes have been characterized as DDTC's "cloud computing" rule, it remains to be seen whether companies with significant ITAR exposure will be able to use commercial cloud computing platforms to store or transmit ITAR-controlled technical data.

In many cases, ITAR-controlled technical data and software are also subject to Defense Federal Acquisition Regulations ("DFARS") cybersecurity and access control requirements that go beyond the FIPS 140-2 standard (*e.g.*, the requirement to meet the more stringent NIST 800-171 requirements). These DFARS provisions do not have similar provisions that exclude foreign national access to encrypted data from the definition of "access."

Thus, many ITAR-regulated companies may continue to use "government cloud" solutions that offer additional NIST standards compliance and limit data storage to the United States, and data access to U.S. person employees of cloud service providers. Further, the terms and conditions of commercial cloud services may continue to prohibit the use of the service to store ITAR-controlled technical data and software, as service providers may be slow to adapt to these changes and/or may be concerned about lingering liability that could arise from the prohibitions on exports to arms-embargoed countries and Russia.

These changes may be more beneficial to smaller companies who perform ITAR-regulated work, but who are not subject to the DFARS requirements because they are not doing work as a DoD prime contractor or subcontractor. They may be able to expand their ability to use non-"government cloud" solutions for storage and transmission of ITAR-regulated technical data and software.

The establishment of a clear ITAR encryption standard will also help companies be better able to demonstrate that no "release" occurs to a foreign national who has general access to an IT system, provided that any ITAR technical data or software remains adequately encrypted. While DDTC has moved in the direction of requiring the actual visual inspection of technical data by a foreign national for a deemed export to occur, it will be easier to prove if adequate encryption of the data can be demonstrated.