wiley

ALERT

U.S. State Department Opens the Door to Use Encryption Carve-Out to Send and Store ITAR Data

December 27, 2019

On December 26, 2019, the U.S. State Department's Directorate of Defense Trade Controls (DDTC) issued its much-anticipated "end-to-end encryption" rule carving out from DDTC's normal licensing requirements appropriately secured technical data controlled by the International Traffic in Arms Regulations (ITAR) that transits and/or is stored abroad. The interim final rule addresses a major practical risk area faced by the U.S. defense industry, as data sent or stored on commercial email or cloud-based solutions may transit a foreign country's internet service infrastructure en route to its final destination or be stored in a foreign country, unbeknownst to the sender and, under the current regulations, in potential violation of the ITAR.

DDTC originally proposed this rule in June 2015, and it is a companion to the rule that the Commerce Department already has in place for technology controlled by the Export Administration Regulations. While this holiday gift to U.S. defense companies may alleviate many current challenges faced by the industry, the rule is not effective until **March 25, 2020**. DDTC is accepting comments on the interim final rule until January 27, 2020, so the final parameters may be modified, but below is a summary of the new carve-out in its current form.

ITAR data transfers meeting the following requirements are not considered to be "exported" for purposes of the regulations and, therefore, do not require DDTC authorization:

- The data that is sent, taken, or stored abroad must be unclassified.

Authors

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Michael D. Faucette
Partner
202.719.4587
mfaucette@wiley.law

Practice Areas

Export Controls and Economic Sanctions
International Trade

- The unclassified data must be secured using "end-to-end encryption," meaning that the data must be encrypted between the sender's in-country security boundary and the recipient's in-country security boundary without being revealed in clear text or unencrypted form or providing the means of decryption to any third party. Note that the intended recipient must be the originator, a U.S. person in the United States, or a person otherwise authorized to receive the data (*e.g.*, via a license or other ITAR approval).
- Such data must be secured using either cryptographic modules compliant with 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). Currently, other means for securing the data, such as tokenization, are not permissible under this carve-out.
- Additionally, the data cannot be intentionally sent to a person or stored in a Section 126.1 ITAR-prohibited country or Russia, nor can such data be sent from a proscribed country or Russia. Note that data in transit via the internet—*i.e.*, incidental collection by a foreign intelligence service or transient storage that is incidental to sending information via the internet—is not deemed to be stored for these purposes; however, long-term storage in a proscribed country or Russia, such as what is commonly done on email servers, is prohibited. Currently, ITAR Section 126.1 countries include Afghanistan, Belarus, Burma (Myanmar), the Central African Republic, China, Cuba, Cyprus, Democratic Republic of the Congo (DRC), Eritrea, Haiti, Iran, Iraq, Lebanon, Libya, North Korea, Somalia, South Sudan, the Republic of the Sudan, Syria, Venezuela, and Zimbabwe. Before relying on this carve-out, it is important to take care and conduct appropriate due diligence to ensure that any services provided by third parties, such as cloud services, are compliant with these restrictions.

U.S. persons are permitted to access the unencrypted version of the data while in the United States without authorization from DDTC. Most U.S. persons employed by ITAR-registered companies also will be able to access the unencrypted data sent using this carve-out for their own use while abroad by relying on the exemption in Section 125.4(b)(9) of the ITAR.

With respect to foreign person access, DDTC clarified that authorization for a release of technical data to a foreign person is required *before* providing access information (*e.g.*, decryption keys, network access codes, passwords) to that foreign person, if the access information can *cause or enable* the foreign person to access, view, or possess the unencrypted technical data. DDTC has warned that without such authorization, "the provision of access information to a foreign person is a violation of ITAR §127.1(b)(1) for failure to abide by a rule or regulation contained in [the ITAR]." DDTC also noted that "causing or enabling a foreign person to access, view, or possess unencrypted technical data may constitute a separate violation of ITAR §127.1(a)" if the exporter has not received authorization from DDTC, because the transfer would be considered an "export" that did not meet the end-to-end encryption carve-out. As such, U.S. exporters should exercise caution and ensure that all of the requirements above are satisfied before relying on this new carve-out.

Wiley Rein has unparalleled export control and national security experience. Should you have any questions regarding this new ITAR rule, please do not hesitate to contact one of the attorneys listed on this alert.