Foreign ITAR cloud storage now permitted

International Trade Alert

4 February 2020
By: Thomas M. deButts | Thomas Reynolds

On December 26, 2019, the Directorate of Defense Trade Controls (DDTC) issued an interim final rule[1] defining "activities that are not exports, reexports, retransfers, or temporary imports" to include certain offshore electronic transmissions or storage of unclassified technical data controlled for export under the International Traffic in Arms Regulations (ITAR) when properly encrypted utilizing end-to-end encryption.

This definition ("activities that are not exports, reexports, retransfers, or temporary imports") will be a new provision in the ITAR (§ 120.54)[2] and aligns it with a similar exemption in the Export Administration Regulations (EAR) (§ 734.18).

Once this interim final rule becomes effective, parties may send, take or store unclassified ITAR technical data via foreign communications infrastructure when it is effectively encrypted using end-to-end encryption.[3] The encryption must be accomplished in a manner that is compliant with the US National Institute for Standards and Technology (NIST) 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 NIST publications. Alternatively, the encryption must meet or exceed an Advanced Encryption Standard (AES) 128-bit (AES-128) security strength. Furthermore, the technical data may not be intentionally sent to a person in or stored in an ITAR § 126.1 country[4] or the Russian Federation. In short, the technical data must be continuously encrypted while outside the United States or until decrypted by an authorized intended recipient.

While this may provide ITAR-registered companies some flexibility with the virtual storage and transmission of their

technical data, **using non-US based cloud storage is still not without risk**. DDTC has clarified that if the technical data is decrypted by someone other than the sender, a US person in the United States, or a person otherwise authorized to receive the technical data, then the technical data would be deemed to never have been secured using the end-to-end encryption meeting the proposed § 120.54(a)(5) standard.

Thus, for example, an unintended release of technical data to a foreign hacker, even under an electronic transmission secured by AES-128 security strength encryption, would mean the original transmission may be deemed a release of ITAR-controlled technical data and potentially would be a violation of the ITAR.

These provisions are set to become **effective on March 25, 2020**. After that date, the use of FIPS 140-2 by cloud providers for offshore storage will comply with both the EAR and the ITAR.

DLA Piper is experienced in the ITAR, EAR, and all encryption-related export controls. If you have any questions, please do not hesitate to contact us.

---

[1] https://www.federalregister.gov/documents/2019/12/26/2019-27438/international-traffic-in-arms-regulations-creation-of-definition-of-activities-that-are-not-exports

[2] The definition includes four other items deemed not to be exports, reexports, retransfers or temporary imports, in §§ 120.54(a)(1)-(a)(4), but these changes are not the subject of this client alert.

[3] Specifically, as defined in ITAR § 120.54(a)(5).

[4] Currently: Afghanistan, Belarus, Burma, Central African Republic, China, Cuba, Cyprus, Democratic Republic of Congo, Eritrea, Haiti, Iran, Iraq, Lebanon, Libya, North Korea, Somalia, South Sudan, Sudan, Syria, Venezuela, and Zimbabwe.

AUTHORS

Thomas M. deButts
Partner
Washington, DC | T: +1 202 799 4000
thomas.debutts@dlapiper.com

Thomas Reynolds
Associate
Washington, DC | T: +1 202 799 4000
tom.reynolds@dlapiper.com