State Dept. Adopts ITAR Amendment on Use of End-to-End Encryption in International Data Transmissions

03.04.2020

The State Department has adopted an important new ITAR amendment confirming that if controlled technical data is encrypted using end-to-end encryption, the transfer of such data outside the U.S. is not considered an export and does not require an export license if it meets the requirements under the amendment. This provides great flexibility and regulatory relief for companies in managing ITAR-controlled technical data on a worldwide basis, including in a foreign cloud environment.

The amendment establishes a new ITAR §120.54 that describes activities that do not constitute exports, reexports, retransfers or temporary imports.[1] On September 1, 2016 the Commerce Department adopted a similar regulation in the effort to provide clarity regarding the international transfer and storage of technology and software controlled under the Export Administration Regulations (?EAR?). At that time, State issued a proposed regulation involving end-to-end encryption but never issued the final rule until now. The intent behind the current amendment is to harmonize the requirements under the ITAR and the EAR.

Under the new amendment, the transfer of ITAR-controlled technical data outside of the U.S. is not considered to be an ?export? for purposes of ITAR compliance if it meets the following requirements:

(i) It is unclassified;

(ii) It is secured using end-to-end encryption;

(iii) It is 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); and

(iv) It is not intentionally sent to a person in or stored in a ?proscribed? country identified in ITAR §126.1 or the Russian Federation, and is not sent from a §126.1 ?proscribed? country or the Russian Federation.

The term ?end-to-end encryption? is defined in the amendment 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.

State also provided guidance regarding the encryption process to be utilized in the Federal Register release accompanying the amendment:

The cryptographic protection must be applied prior to the data being sent outside of the originator?s security boundary and remain undisturbed until it arrives within the security boundary of the intended recipient. For communications between individuals, this can be accomplished by encrypting the data on the sender?s computer prior to emailing or otherwise sending it to the intended recipient. For large entities, the security boundary may be managed by IT staff, who will encrypt the data before it leaves the entity?s secure network and decrypt it on the way into the network. However, in all instances, the means of decryption must not be provided to any third party and the data must not have the cryptographic protection removed at any point in transit.[2]

Despite the benefits of the amendment, exporters should be alert to a number of risks that may arise in the application of the new regulation. For example, the technical data must remain continuously encrypted while outside the United States or until decrypted by an authorized intended recipient ? if the technical data is decrypted by someone other than the sender, a U.S. person in the United States, or a person otherwise authorized to receive the technical data, then the technical data is not considered secured.[3] Also as referenced above, the data cannot be intentionally sent to a person in or stored in a ?proscribed? country identified in ITAR §126.1 or the Russian Federation, and cannot be sent from such countries.

During the rulemaking process one party submitted a comment with a recommendation to simplify the process of storing controlled data in the cloud, suggesting that State provide a ?safe harbor? by only requiring that cloud customers obtain contractual assurances that the data would not be stored in a §126.1 country or the Russian Federation. However State rejected this suggestion, stating that it was not in the national security interests of the United States. The agency stated: ?The Department recognizes it can be difficult to control the actions of third parties, including partners, service providers,

and subcontractors, and will review potential violations on a case-by case basis, subject to the totality of the facts and circumstances comprising the issue at hand.? (Emphasis added.)[4] Thus companies are put on notice of the risk of potential violations if cloud storage arrangements are not set up properly and the importance of conducting thorough due diligence regarding foreign cloud providers in setting up such arrangements.

The new amendment will become effective on March 25, 2020.

As with other ITAR exemptions, the new amendment provides significant benefits for companies in their ITAR compliance activities, provided they carefully meet the terms and conditions of the exemption.

ADDITIONAL RESOURCES

Other Articles You May Be Interested In:

- Export Control Laws For The General Counsel
- ITAR For Government Contractors
- ITAR Compliance Checklist
- Dealing With Violations In Export and Import Transactions

Note: This article contains general, condensed summaries of actual legal matters, statutes and opinions for information and education purposes. It is not intended and should not be construed as legal advice.

To be placed on our list to receive additional articles on export and import law please **click here**. Should you have any questions on this topic or others related to import/export law, please contact Thomas McVey at: tmcvey@williamsmullen.com or 202.293.8118. Additional articles on ITAR, EAR and US sanctions programs are available at: ?**Export Articles.**?

[1] See Department of State, International Traffic In Arms Regulations, Interim Final Rule and Request for Comment: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports; Creation of Definition of Access Information; Revisions to Definitions of Export, Reexport, Retransfer, Temporary Import, and Release, 84 Federal Register No.247, December 26, 2019 (the ?Interim Final Rule.?)

[2] See Interim Final Rule p. 70889.

[3] Id.

[4] Id.

Related People

Related Services

- ITAR, Export Controls and Economic Sanctions
- International Trade and Business