Summary of Changes to International Traffic in Arms Regulations - Encryption Rule

OVERVIEW: On December 26, 2019, the Directorate of Defense Trade Controls (DDTC) published an ITAR interim final rule (84 FR 70887, effective March 25, 2020) creating a new definition of activities that are not exports, reexports, retransfers, or temporary imports. It consolidates in one location several previously existing but disassociated activities that are not considered exports and adds a new entry for properly secured unclassified technical data in an encrypted state. This rule is compatible with, but not identical to, the analogous provision in the Export Administration Regulations (EAR) 15 CFR parts 730 through 774. It also provides the regulatory framework for control of properly secured encrypted technical data and its means of decryption.

The rule does the following:

- Adds new ITAR § 120.54 to describe "activities that are not exports, reexports, retransfers, or temporary imports" (an otherwise "controlled event") and do not require authorization from DDTC. The first four activities not considered to be controlled events are:
  - launching items into space (formerly § 120.17(a)(6))
  - transmitting or transferring technical data to U.S. persons within the United States
  - transmitting or transferring technical data between or among U.S. persons within a single foreign country
  - moving a defense article between the states, possessions, and territories of the United States

- The fifth activity, and the reason this is referred to as the "Encryption Rule," is the sending, taking, or storing of technical data that is:
  - unclassified;
  - secured using end-to-end encryption as prescribed;
  - not intentionally sent to a person in or stored in countries subject to restrictions under ITAR § 126.1 or the Russian Federation; and,
  - not sent from a § 126.1 country or the Russian Federation.

- Revises the definitions of export, reexport, retransfer, and temporary import to accommodate the new definition.

What can I do as of March 25, 2020, that I couldn't do before?

If you properly secure your unclassified technical data using the minimum encryption standards provided, you can take or send that data out of the U.S. or between other countries, and the action may not require a license.

There are only a few things to remember:

1. Meet or exceed the standard

2. Watch out for 126.1 countries and the Russian Federation

3. Keep it end-to-end encrypted.

Summary of Changes to International Traffic in Arms Regulations - Encryption Rule

- Adds ITAR § 120.55 to define "access information" and revises the definition of "release" at § 120.50 to manage the method by which properly secured encrypted information may be decrypted. The revisions to § 120.50 also clarify when such decryption results in a controlled event; meaning that an export, reexport, retransfer, or temporary import has occurred.
  - Access information is defined as information that allows access to encrypted technical data in an unencrypted form (e.g., decryption keys, network access codes, and pass codes).
  - The definition of release is expanded to include the use of access information to:
    - cause or enable a foreign person to access, view, or possess technical data; or,
    - cause technical data outside of the United States to be in an unencrypted form.
- Adds a new paragraph (b) to the definition of release at § 120.50 to clarify that a U.S. person does not need to obtain a specific authorization from DDTC to provide access information to a foreign person in order for that foreign person to access technical data in an unencrypted form, *provided the foreign person is otherwise authorized to receive the technical data*. If no other authorization exists for the foreign person to access the technical data, the provision of the access information by the U.S. person is a violation of the terms of § 120.50.

Does this mean I can put all my ITAR stuff 'on the cloud' as of March 25, 2020? Not all your ITAR stuff. This only applies to unclassified technical data. Classified technical data is not covered by new ITAR § 120.54, no matter the type of encryption. Also, know your cloud provider and where they operate. New ITAR § 120.54 doesn't cover storage in countries subject to restrictions under ITAR § 126.1 or the Russian Federation. Finally, remember to wait until March 25, 2020.

It's after March 25, 2020, I've got properly encrypted unclassified ITAR tech data and I want to let a foreign person access that technical data. Do I need a license to send the access information to the foreign person so they can access it? No. You don't need to ask DDTC for permission to send the access information to the foreign person. However, the actual access of that technical data in an unencrypted form is an export (or other controlled event) and there needs to be an authorization (e.g., license, agreement, or applicable exemption) for the export of that technical data to that foreign person. If you send access information to a foreign person and there is no authorization to release that technical data to them, it's a violation.

How do I know if my technical data is "properly secured" using "end-to-end encryption"? Revisions to ITAR § 120.54 or referenced standards may supersede this document, but the data needs to be secured using FIPS 140-2 standard in accordance with National Institute for Standards and Technology (NIST) guidance, or by other methods that are at least comparable to the minimum AES 128 bits security strength (see "Table 2: Comparable strengths" of NIST Special Publication 800-57 Part 1, Revision 4, at page 53). Users should document the encryption's effectiveness prior to use.