Published on *The National Law Review* https://natlawreview.com

New ITAR End-To-End Encryption Rule Will Promote Efficient Defense Technical Data Storage and Transmission, But Some Risks Remain

Article By:

Ivan W. Bilaniuk

Tony M. Busch

Unclassified defense technical data that is properly secured with end-to-end encryption is no longer considered an export when it is transmitted outside the U.S., as of March 25, 2020. Access to the unencrypted data by an unauthorized foreign person, however, remains an ITAR-controlled export. This change resulted from an Interim Final Rule coming into effect from the U.S. Department of State Directorate of Defense Trade Controls (DDTC) that amended the International Traffic in Arms Regulations (ITAR).

The new ITAR rule amends the definition for "activities that are not exports, reexports, retransfers, or temporary imports," to include the transmission of unclassified defense technical data utilizing end-to-end encryption.[1] Specifically, the rule states that it is not an "export" under the ITAR to send, take, or store unclassified "technical data" – information and software required for all aspects of a defense article's life cycle from design through operation, maintenance, and modification – if the technical data is secured using end-to-end encryption meeting the National Institute for Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) Publication 140-2, or a comparable minimum 128-bit security strength encryption algorithm. (22 CFR § 120.54(a)(5); *see also* § 120.54(c)).[2]

The ITAR encryption rule change releases the end-to-end encrypted data transmission from ITAR control, but the unencrypted defense technical data within that encrypted transmission remains ITAR-controlled. Thus, parties will be strictly liable if "access information" is used to "release" unencrypted technical data outside the U.S. or to a foreign person not authorized to receive the data. "Access information" is defined to include decryption keys, network access codes, and passwords. In addition to the pre-existing definitions of a "release,"[3] the new rule now also defines a "release" as the use of access information to "cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data," or to "cause technical data outside of the United States to be in unencrypted form". (22 CFR § 120.50(a)(3)-(4)). DDTC cautions that the foreign person has to be authorized to receive the technical data before he or she is provided the access information that will permit accessing the data in an unencrypted state.[4]

This Interim Final Rule substantially aligns the ITAR with the analogous rule in the Export Administration Regulations (EAR), which apply to dual-use exports.[5] For instance, both this new ITAR encryption rule and the existing EAR encryption rule require that technical data crossing security boundaries remains in an encrypted state without the means of decryption being provided to a third party.[6] This alignment is welcome news for companies dealing in defense articles and defense services. It means companies that have already modernized their data storage and transmission policies for technology/technical data subject to the EAR will find they will be able to extend those policies to unclassified ITAR-controlled technical data. In other words, they will be able to streamline their internal data storage and data-sharing practices by moving ITAR-controlled unclassified technical data into the cloud,[7] potentially even with a foreign cloud provider, rather than having to store it separately and locally.

Compliance risks remain with this new ITAR encryption rule, however, such as the following:

1) ***Compliance with export restrictions of U.S. allies.*** This new end-to-end encryption standard enables a more free flow of unclassified defense technical data in compliance with U.S. regulations. Nevertheless, companies holding both U.S. and non-U.S. defense technical data must be cognizant that U.S. allies' regulatory regimes have yet to adopt a similar standard for export of defense technical data; implementing a single cloud-based solution will remain a significant challenge. In responding to comments, DDTC stated that it is working to solve this issue in consultation with its allies.

2) ***Avoiding an unauthorized "release" as broadly defined by the rule.*** The definition of "release" in the rule is very broad, as discussed above. As commenters on the proposed rule pointed out, the new definition could result in violations whenever a foreign national unauthorized person's user account is accidentally provided access credentials for an encrypted network drive containing unclassified defense technical data, even if that person never actually accesses the data or even knew they had been granted such access.[8] DDTC has insisted in the past "that theoretical or potential access to technical data is not a release,"[9] but companies should proceed with caution given the new broad definition of "release."

3) ***Compliance with restrictions on transiting through or being stored in the Russian Federation or a list of proscribed countries***. It is not a violation for end-to-end encrypted unclassified defense technical data that is in transit through the internet to be transiently *and* unintentionally stored in Russia or an ITAR-proscribed country[10] by virtue of being data in transit through the internet.[11] But storage in these countries or transmission of such data from these countries does constitute a violation. Such a violation carries strict liability, so even a contractual assurance from a counterparty expressly warranting that no storage will occur in Russia or a § 126.1 country is insufficient protection.[12] DDTC does note in the Interim Rule that it "will review potential violations on a case-by-case basis, subject to the totality of the facts and circumstances . . . ,"[13] in acknowledgement of the difficulty of controlling the actions of third parties such as service providers and subcontractors.

Given the rule came into force as an interim final rule, it is still possible DDTC will fine-tune the rule further. If you have questions about this encryption rule's effect on your operations or have other ITAR or EAR export compliance questions, contact Ivan W. Bilaniuk or your Dinsmore attorney.

---

[1] 84 FR 70887 ("Interim Final Rule") at 70887-93.

[2] The new ITAR rule also lists four other categories of activities that are not exports, reexports, retransfers, or temporary imports, but which are not the focus of this article: (1) the launching of items into space; (2) the transmission/transfer of technical data between U.S. persons in the United States; (3) the transmission/transfer "within the same foreign country [of] technical data between or among only U.S. persons . . . ," so long as end-user prohibitions are not otherwise violated; and (4) the shipment, movement, or transfer of defense articles within the U.S. (22 CFR § 120.54(a)(1)-(4)).

[3] 22 CFR § 120.50(a)(1)-(2).

[4] Interim Final Rule at 70890-91 (emphasis added).

[5] S*ee* 15 CFR § 734.18 (defining certain end-to-end encryption data transmission as "activities that are not exports, reexports, or transfers" under the EAR).

[6] *Compare* 22 CFR § 120.54(b)(1) *with* 15 CFR § 734.18(b).

[7] Interim Final Rule at 70888-89 ("a controlled event does not occur when technical data is encrypted prior to leaving the sender's facilities and remains encrypted until decrypted by the intended authorized recipient or retrieved by the sender, as in the case of remote storage").

[8] Ltr. from CompTIA, Jan. 24, 2020, at 2 (Dkt. No. DOS-2019-0040-0003, posted Feb. 5, 2020); Ltr. from Aerospace Industries Association at 1-3 (Dkt. No. DOS-2019-0040-0002, posted Feb. 5, 2020). *See generally* 22 CFR 120.50(a)(3)-(4) & (b).

[9] *See* International Traffic in Arms: Revisions to Definition of Export and Related Definitions 81 FR 62004, 62005 (Sept. 8, 2016) (revising definitions in ITAR at 22 CFR Parts 120, 125, 126, and 130).

[10] ITAR-proscribed countries are those countries listed in 22 C.F.R. § 126.1 to which export of defense articles, defense services, and defense technical data are prohibited.

[11] 22 CFR § 120.54(a)(5)(iv) ("Not intentionally sent to a person in or stored in a country proscribed in §126.1 of this subchapter or the Russian Federation"), Note to (a)(5)(iv) ("Data in-transit via the internet is not deemed to be stored") & (a)(5)(v)). *See also* Interim Final Rule at 70889 ("One commenter requested that the Department clarify that appropriately encrypted transmissions may transit the Russian Federation or a § 126.1 country and still qualify for this provision. The Department clarified this point by adding the word ''intentionally,'' to differentiate those electronic transmissions that were intentionally sent to Russia or a § 126.1 country, and those that simply transited them in route to another country.").

[12] Interim Final Rule at 70889.

[13] *Id.*

National Law Review, Volume X, Number 91

Source URL:https://natlawreview.com/article/new-itar-end-to-end-encryption-rule-will-promote-efficient-defense-technical-data