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

U.S. State Department Changes Export Control Requirements for Secure Handling of Defense Technical Data, Easing Burden on U.S. Industry

Article By:

Nate Bolin

On December 26, 2019, the U.S. State Department's Directorate of Defense Trade Controls (DDTC) announced it is amending the International Traffic in Arms Regulations (ITAR) to exclude certain secure transfers of defense technical data from export licensing requirements. The amendments become effective on March 25, 2020. Provided they are careful to meet the specific technical and other requirements of the new regulations, U.S. companies and their overseas partners that are engaged in ITAR-controlled activities will see significant benefits and reduced burdens in the secure handling and storage of electronic data. This change will also more closely align ITAR requirements for handling of electronic technical data with those of the Export Administration Regulations (EAR), further easing export control compliance burdens on industry.

Prior to the latest rule change, any transmission or storage of ITAR-controlled technical data outside of the United States or to non-U.S. persons required a specific license or other approval from DDTC. This imposed a significant burden on U.S. industry, since even the secure, encrypted transmission or electronic storage outside the United States (such as on a cloud-based server) of ITAR technical data would trigger a licensing requirement – even if such data were never accessed or used. Further, the prior ITAR rules contrasted sharply with EAR rules that permit such electronic transmission or storage of EAR-controlled technology without a license so long as certain encryption and other requirements are met.

The latest ITAR rules will change this. Effective March 25th, provided that the following requirements are met, the secure transmission or storage of ITAR technical data outside the United States will not be treated as an export and will not require prior DDTC approval. Specifically, to be eligible for license-free treatment, the transmission or storage of ITAR technical data must:

1. Be conducted via "end-to-end" encryption that meets the U.S. National Institute of Standards and Technology (NIST) Federal Information Processing Standards of Publication 140-2 (FIPS 140-2) or otherwise meet or exceed a 128-bit encryption strength as specified in the DDTC rule;[1]

2. Not be intentionally sent to or stored in Russia, China, or any other country identified in Section 126.1 of the ITAR (a list that also includes most countries subject to U.S. economic

sanctions, such as Cuba and Iran);[2] and

3. Not be viewed or accessed by anyone who is not eligible to view or receive ITAR technical data (e.g., a non-U.S. person not authorized by a license or a person on a U.S. government denied party list). Note that under the new rules, it is a violation of this last requirement to provide a non-authorized person with a password or other means that can cause or enable unauthorized access to the encrypted data.

Notably, these changes apply regardless of whether the transmission or storage is made securely via a telecommunication network or via a properly encrypted laptop or other physical storage device. However, all transmission and storage must not result in a release of unencrypted technical data to an unauthorized person, such as a non-licensed foreign person.

In addition to the above changes, the latest rule clarifies a number of related areas and issues that should further ease the compliance burden on industry:

- First, the rule reemphasizes that an exchange of ITAR technical data between U.S. persons in the United States (including between different locations within the United States) is "unequivocally" not an "export" or other "controlled event" and does not require an ITAR license or other approval – even if the data are not encrypted. Having said that, the rule cautions that any release of such data to a non-U.S. person (even in the United States) would be a "controlled event" and would require a license.

- Second, the rule makes clear that an exchange of ITAR technical data solely between U.S. persons in the same foreign country is not a "controlled event" and does not require an ITAR license. Any release of such technical data to a non-U.S. person would, however, require a specific license or other approval. While this clarification means that U.S. persons overseas can now have greater comfort that their exchanges of ITAR technical data inside the same country (such as at a project worksite) will not require further authorization, great care is warranted to ensure that such data are not inadvertently released to foreign persons. To this end, companies engaged in overseas projects should carefully review their operational and security requirements related to the protection of company data and systems.

- Third, the rule specifies that ITAR licensing requirements do not apply to any non-U.S. origin defense technical data that merely transit or are stored in the United States without being accessed, provided that such non-U.S. origin data are (i) encrypted in accordance with the encryption standards set forth above, (ii) do not originate in Russia, China, or another Section 126.1 country, and (iii) are not sent to any such countries. This clarification should reduce industry concerns about "incidental" transmission of secured foreign defense data via U.S. telecommunications networks.

The latest ITAR changes will make it possible for U.S. companies and their authorized overseas partners to handle the secure transmission and storage of ITAR technical data in much the same way that they currently treat EAR-controlled technology. This promises to reduce licensing, compliance, IT, and administrative costs and should significantly benefit industry over the long-term. Companies involved in ITAR-regulated activities should carefully review the latest regulations and consider whether updates to their own systems, policies, and procedures may be warranted to take advantage of the latest rule changes when they become effective on March 25, 2020.

For more information on the ITAR, U.S. export controls, and the latest changes to these regulations, please contact the author or your regular Drinker Biddle contact.

[1] Notably, the DDTC commentary on the rule changes also allows for decrypting of data within a secure firewall or other “security boundary” as well as anti-virus scans of the encrypted data, so long as unauthorized persons do not gain the ability to access or view the data in clear text form.

[2] DDTC has specified that temporary storage of properly encrypted ITAR technical data in these countries that is merely incident to Internet transmissions (such as email) does not constitute an “intentional” transmission or storage that would violate the rule. However, long-term storage of such technical data in these countries, such as would commonly occur on email servers, is prohibited. Accordingly, companies seeking to utilize the new rule should take care to ensure that their data is not stored on email servers or other such “long-term” storage in Section 126.1 countries. In selecting service providers or systems to implement the new rule, appropriate contractual and audit provisions to ensure compliance with this requirement are strongly recommended.

National Law Review, Volume X, Number 10