



January 24, 2020

Comments submitted via the Federal eRulemaking Portal: <http://www.regulations.gov>

Ms. Sarah Heidema
Director
Office of Defense Trade Controls Policy
Department of State
2201 C St. NW
Washington, D.C. 20520

Subject: ITAR Amendment—Revisions to Definitions; Data Transmission and Storage

Reference: RIN 1400–AE76 – Federal Register / Vol. 84, No. 247 / Thursday, December 26, 2019 / Interim Final Rule

Dear Ms. Heidema:

On behalf of the Computing Technology Industry Association (CompTIA) and the diverse collection of small, mid-sized, and large technology companies we represent, thank you for the opportunity to provide feedback on the Interim Final Rule modifying, revising, and adding definitions to Part 120 of the International Traffic in Arms Regulations (ITAR) (“the Rule”).

We fully support DDTC’s efforts to harmonize the ITAR with the Export Administration Regulations (EAR) and recognition of effective end-to-end encryption. As members of the IT industry, we are committed to upholding U.S. national security interests and promoting secure transfers of technical data. In general, this Rule is a promising indication to industry of the importance of closely collaborating with the U.S. government on matters of importance to U.S. national security and foreign policy.

Our main concern is limited to the revised definition of “release.” Although CompTIA welcomes the Rule as providing greater flexibility for cloud users and consistency with other regulatory regimes, we have concerns about an apparent expansion of the definition to include cases in which a foreign person does not actually access controlled technical data. New ITAR § 120.50(a)(3) adds the following language to the definition of “release” (emphasis added):

*(3) The use of access information to cause **or enable** a foreign person, including yourself, to access, view, or possess unencrypted technical data;*

New ITAR § 120.50(b) further revises the definition of “release” to include the following (emphasis added):

*(b) Authorization for a release of technical data to a foreign person is required to provide access information to that foreign person, **if that access information can cause or enable** access, viewing, or possession of the unencrypted technical data.*

With regard to the latter provision, DDTC provided the following context in the Interim Final Rule:

The new paragraph (b) clarifies that the provision of access information to a foreign person is not itself a controlled event; there is no need for an application by the access information provider, or for the Department to issue an authorization, for the provision of access information. However, in order for the Department to effectively control the release of technical data to a foreign person in certain circumstances, paragraph (b) requires an authorization for a release of technical data to a foreign person before providing the access information to that foreign person, if that access information can cause or enable access, viewing, or possession of the unencrypted technical data. In the absence of an authorization for the release of technical data in such circumstances, the provision of access information to a foreign person is a violation of ITAR § 127.1(b)(1) for failure to abide by a rule or regulation contained in this subchapter.

Taken together, 120.50(a)(3) and 120.50(b) and the comments in the Rule suggest that it is an ITAR violation for a foreign person to be able to access encrypted technical data subject to ITAR controls while also having access information sufficient to decrypt this data regardless of whether such decryption actually occurs. Such a position is directly inconsistent with DDTC’s clear and unambiguous guidance in a final rule of September 8, 2016 that “theoretical or potential access to technical data is not a release” and that “a release will have occurred if a foreign person does actually access technical data.” International Traffic in Arms: Revisions to Definition of Export and Related Definitions, 81 FR 62004, 62005.

These provisions as they are currently drafted appear to create the possibility for regulatory outcomes inconsistent with the absence of harm to U.S. national security and foreign policy interests. As an example, one can imagine a foreign national employee’s corporate user account being briefly and inadvertently granted access credentials allowing logical access to an encrypted network drive containing ITAR-controlled technical data. Under DDTC’s previous guidance that “theoretical or potential access . . . is not a release,” whether or not this scenario resulted in an ITAR violation would depend upon whether the foreign national actually used these credentials to view technical data within this drive. This is a sensible result considering that no harm to national security has occurred if the foreign national did not, in fact, view the controlled

technical data during this brief period of theoretical access. Under 120.50(a)(3) and 120.50(b), however, these circumstances would result in an ITAR violation -- even if it could be demonstrated that the foreign person did not actually utilize these credentials to view the technical data.

Furthermore, the provisions at issue appear to penalize the use of encryption as a means of securing technical data. If technical data were not encrypted (e.g., saved on unencrypted physical media like a CD-ROM or in physical printed form) and accessible to both U.S. Persons and foreign nationals, presumably this “theoretical or potential access” by a foreign person would not constitute a release. It is only by encrypting the technical data that companies expose themselves to the stricter standards set forth in 120.50(a)(3) and 120.50(b). In a rule that otherwise promotes the role of encryption to protect sensitive technical data, these provisions actually create disincentives for using encryption in this way.

CompTIA appreciates that DDTC’s inclusion of 120.50(a)(3) and 120.50(b) may reflect concerns about the agency’s ability to prove in an enforcement context whether a release has or has not occurred -- particularly where there is insufficient access logging data to reach a factual determination on this point. However, 120.50(a)(3) and 120.50(b) apply even where access logging is sufficiently robust to demonstrate that no access by the foreign person actually occurred.

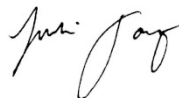
For the reasons set forth above, CompTIA respectfully requests that DDTC clarify the language in 120.50(a)(3) and 120.50(b) to be consistent with the agency’s stated position that theoretical or potential access is not a release. This could be accomplished, for instance, by striking “or enable” from 120.50(a)(3) and replacing “if that access information can cause or enable” in 120.50(b) with “if the provision of that access information results in.”

We appreciate DDTC’s efforts to provide greater clarity to Part 120 of the ITAR and the opportunity to provide feedback. We hope to continue engaging with you on this matter and collaborating to ensure that U.S. national security interests are upheld in the course of our business.

Sincerely,



Ken Montgomery
Vice President, International Trade
Regulation & Compliance



Juhi Tariq
Senior Manager, International Trade
Regulation & Compliance