wiley

ARTICLE

State and Commerce Publish Much Anticipated Proposed Rules Revising Certain ITAR and EAR Definitions

June 19, 2015

Continuing their hot streak of progress pursuant to the President's Export Control Reform (ECR) Initiative, the Department of Commerce's Bureau of Industry and Security (BIS) and Department of State's Directorate of Defense Trade Controls (DDTC) recently published proposed rules updating and revising certain key terms in the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR), respectively. The proposed rules address a host of important definitions, most notably "technology," "technical data," "public domain," "fundamental research," and "export," and make a number of additional changes.

A major goal of the ECR Initiative is the harmonization, where possible and practical, of definitions and terms used across both regulatory schemes. The proposed rules published on June 3, 2015 mark an important step in this process, but still include some ambiguities and inconsistencies.

"Technical Data" and "Technology"

DDTC proposes harmonizing the definition of "technical data" with that of the EAR's "technology." More specifically, the revised definition of "technical data" would include information required for the development, production, operation, installation, maintenance, repair, overhaul, or refurbishing of a "defense article." The EAR's definition of "technology," meanwhile, would maintain its references to development, production, and use. Additionally, BIS's "technology" definition and DDTC's "technical data" definition would also include information that would allow access to "technology/technical data" in

Authors

John R. Shane
Partner
202.719.7222
jshane@wiley.law

Lori E. Scheetz
Partner
202.719.7419
lscheetz@wiley.law

Practice Areas

International Trade

clear text or "software," like decryption keys, network access codes, or even passwords.

While DDTC's proposed "technical data" definition represents the more significant structural change between the two terms, BIS also proposes to adjust its "technology" definition in a nod to the ITAR to include an explicit carve-out for non-proprietary general system descriptions, information on the basic function or purpose of an item, and certain telemetry data.

Further, in revising the definitions for "technical data" and "technology," DDTC's and BIS's proposed rules also address the definitions for "required" and "peculiarly responsible." DDTC's proposed rule would create a definition for "required," which would be aligned with the EAR's definition of the term: DDTC's definition would specify that only the portion of "technical data" peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions would be controlled. DDTC also proposes to include notes to assist with the application of its "required" definition, including one that would establish a test for determining whether information is peculiarly responsible for meeting or achieving the controlled performance levels, characteristics, or functions of a particular "defense article" and which would mirror the catch-and-release format currently employed in the definition for "specially designed." While BIS's "required" definition would remain largely unchanged, BIS also proposes adding clarifying notes and related examples to address frequently asked questions encountered by the agency. BIS's "peculiarly responsible" definition would also reflect the catch-and-release structure of the "specially designed" definition.

"Public Domain" and "Fundamental Research"

DDTC's proposed rule would also include a revised definition of "public domain" specifically drafted to address the continually evolving array of media (*e.g.*, the Internet) through which information can be disseminated and shared. Information would be deemed available in the "public domain" where it is made available to the public without restrictions on its further dissemination. However, much to the chagrin of industry, parties must obtain the U.S. government's (USG) authorization prior to releasing any "technical data" or software subject to the ITAR into the "public domain." Application for such authorization would be made to either DDTC, the Department of Defense's Office of Security Review, a relevant USG contracting authority with sufficient authority to allow the "technical data" or software to be made available to the public (if such an authority exists), or another USG official with authority to allow the "technical data" or software to be made available to the public. DDTC claims that this requirement is not new, but it has already been met with grumbling from members of the private sector.

Additionally, DDTC's proposed rule would clarify that information excluded from the definition of "defense article" is not "technical data," and therefore does not require USG authorization prior to its release into the "public domain." Such information would include information arising during or resulting from "fundamental research;" general scientific, mathematical, or engineering principles commonly taught in schools; and information that is contained in patents. Further, dissemination of "technical data" or software made available without USG authorization constitutes a violation only if done with knowledge that the "technical data" or software was made publicly available without prior authorization.

DDTC's proposed rule also includes a separate definition for "technical data that arises during, or results from, fundamental research." DDTC describes this category of information as "conceptually distinguishable" from information captured in the revised "public domain" definition, and the expanded definition now would include research funded in whole or in part by the USG. BIS has also revised its definition of "fundamental research," but its revisions appear mostly cosmetic and are not intended to change the definition's scope.

"Export"

Both BIS's and DDTC's proposed rules include revised definitions of "export." DDTC's revised "export" definition would be better aligned with the EAR's definition of the term. Generally, the scope of covered activities would remain the same,[1] though the revised definition specifies that the release or transfer of information securing technical data or software (*e.g.*, decryption keys, passwords, network access codes, etc.) constitutes an export. This change allows for the idea that the provision of certain encrypted technical data would not be an export under certain circumstances. Further, the act of providing the means to access ITAR-controlled technical data or software will be an ITAR-controlled event, even absent specific knowledge that a foreign national has or will access that data or software.

Like DDTC's proposed rule, BIS's proposed rule would specify that release or transfer of the means of accessing technology in clear text or software constitutes an export. However, unlike the ITAR, where the mere ability to access data or software is an issue, providing the means to access EAR-controlled technology or software will not be an EAR-controlled event unless done with "knowledge" that such provision will cause or permit the transfer of controlled technology in clear text or software to a foreign national.

Additional Changes

Notably, both agencies also addressed activities that would not be considered exports, reexports, or transfers. The proposed rules appear to recognize at least some of the nuances involved with modern data storage, cloud services, and email, issues industry has raised for quite some time. Recognizing that email may transit through a foreign country's infrastructure en route to its final destination and that information stored on the cloud may be stored on servers located in a foreign country without the sender's knowledge, DDTC's proposed rule would create an exclusion from the definition of export that covers the transmission and storage of encrypted, unclassified technical data and software. The technical data or software must be secured using end-to-end encryption and cryptographic modules that are compliant with the U.S. National Institute for Standards and Technology's (NIST) Federal Information Processing Standards (FIPS) Publication 140-2 and supplemented with controls in accordance with current NIST publication guidance. Encrypted data also cannot be stored in a 22 C.F.R. § 126.1 country or Russia. BIS's proposed rule includes a similar carve-out from the definition of "export," but would allow for the transmission of technology protected using cryptographic means that are similarly effective to NIST FIPS Publication 140-2 compliant methods without requiring certification of those means.

DDTC's proposed rule also includes still more changes to the proposed revised definition of "defense services," marking the third set of additions and edits to the definition since the kick-off of the ECR Initiative. This most recent proposed rule would specify that certain activities (*e.g.*, intermediate- or depot-level maintenance) generally are not "defense services" if performed by a person who does not have, prior to the performance of the services, knowledge of the U.S.-origin technical data directly related to the defense article that is the subject of the assistance. Further, among other changes, in addition to excluding from the definition of defense services the installation of any item into a defense article, the revised definition also would exclude from this definition the installation of a defense article into any item.

* * *

As with their other proposed rules, BIS and DDTC are encouraging industry members to submit comments. Both BIS and DDTC seek industry feedback from industry regarding a number of issues, including the proposed rules' treatment of methods and manners of data transmission, storage, and access; and the alignment of and/or contradictions created by the proposed revisions. Comments should be submitted by August 3, 2015, and can be filed either by direct submission to the relevant agency or via the Federal eRulemaking Portal at http://www.regulations.gov.

For the full text of the proposed rules and a complete list of the proposed changes, please refer to DDTC's proposed rule here and BIS's proposed rule here.[2]

---

[1] DDTC's proposed revised "export" definition also clarifies that the release of technical data or software to a foreign person is deemed to be an export to all countries in which the foreign person has held citizenship or permanent residency, consistent with DDTC's long-standing practice. In contrast, BIS's revised "export" definition would codify its deemed export rule by specifying that the release of technology or source code to a foreign national is deemed to be an export to the person's *most recent* country of citizenship or country of permanent residence.

[2] *International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions*, 80 Fed. Reg. 31,525 (Dep't State June 3, 2015) (proposed rule); *Revisions to Definitions in the Export Administration Regulations*, 80 Fed. Reg. 31,505 (Dep't Commerce June 3, 2015) (proposed rule).