COVINGTON

State and Commerce Departments Propose Revisions of Key Export Control Definitions

June 12, 2015

International Trade Controls

On June 3, 2015, the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC") and the U.S. Department of Commerce, Bureau of Industry and Security ("BIS") issued a pair of proposed rules (80 Fed. Reg. 31525 and 80 Fed. Reg. 31505) that would amend, respectively, the International Traffic in Arms Regulations ("ITAR") and the Export Administration Regulations ("EAR") to revise and harmonize certain key definitions. The proposed rules contain two major changes. First, both rules propose to decontrol certain transfers of encrypted technology, technical data, and software. These are long-awaited proposals to address concerns that have developed as the technology for electronically transmitting and storing data has expanded, including with the addition of cloud technology. The second major development is the proposal by DDTC of a new definition of "defense service" that would narrow the scope of activities that are regulated services under the ITAR.

A variety of other revisions are proposed to key export control terminology through new or revised definitions, or the use of explanatory notes to regulatory provisions. These include revisions to or elaborations of such foundational terms as "technology," "technical data," and "required"; "export," "release," "reexport," and "retransfer"; and "published" and "public domain," among others. Many of the changes are intended primarily to clarify and harmonize the definitions to make them more consistent between the ITAR and EAR. The agencies have published a chart comparing the proposed regulatory text in the two rules. A copy of the chart is available here.

DDTC and BIS will accept comments on the proposed rules until August 3, 2015.

In another proposed rule issued on May 26, 2015 (80 Fed. Reg. 30001), DDTC has proposed to amend the ITAR to clarify the registration and licensing requirements for the defense services provided by natural U.S. persons who are employed by non-U.S. persons. In particular, the proposed rule clarifies that registration and authorization is required for U.S. persons (including dual nationals of the United States and the non-U.S. employer's country) who provide defense services to or on behalf of their employer. The rule includes a number of provisions that should help mitigate the potential burden of these requirements, but many natural U.S. persons employed outside of the United States and their non-U.S. employers still may be significantly impacted by this new rule.

DDTC will accept comments on this rule until July 27, 2015. DDTC requests comments from current and prospective non-U.S. employers of U.S. persons (including U.S. persons employed as regular employees or long-term contract employees (*i.e.*, for one year or more)), as well as from current or future U.S. person employees and contractors.

Relaxation of Controls on Transmission and Storage of Encrypted Information

In the rules issued on June 3, BIS and DDTC have proposed changes to the treatment of data and software that are encrypted to specified standards. These changes, if implemented, would represent a major relaxation of rules that have long hampered international connectivity and collaboration in global companies. Under current restrictions, transfer of data or software to a server or network location outside the United States constitutes an "export" even if the data or software is encrypted. Likewise, under current rules, providing non-U.S. employees in the United States or non-U.S. offices with the ability to access ITAR-controlled data (even if they do not actually access the data) or with actual access to EAR-controlled data may constitute an "export" even if that data is protected by encryption. Thus, to avoid risk of unlicensed exports, companies must limit access to authorized persons, even when the data's substantive content is encrypted and thus not actually being communicated to persons not authorized to receive the data. The proposed rules would allow companies to store data on servers outside the United States, and make data accessible to non-U.S. offices or to non-U.S. employees in the United States, as long as the data is encrypted to certain standards and not stored in a country subject to a U.S. arms embargo or Russia (though nationals of or offices in such countries could apparently be given access to the server where the data is stored as long as they are not given the ability to decrypt the data, as explained below).

Specifically, the new rules propose to add provisions to both the EAR and the ITAR that define "activities that are not exports, reexports, or transfers." In addition to gathering existing exclusions or carve-outs from these concepts into a single location in the rules, both proposed rules add a new provision stating that exports, reexports, transfers, and retransfers do *not* include "sending, taking, or storing" technology, technical data, or software that is:

1. Unclassified;
2. Secured using "end-to-end" encryption;
3. Secured using cryptographic modules (hardware or software) compliant with Federal Information Processing Standards Publication 140-2 (FIPS 140-2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology publications;[1] and
4. Not stored in the Russian Federation, or in the group of countries listed in the EAR's Country Group D:5 or proscribed in ITAR § 126.1.

The proposed rules define "end-to-end encryption" as the provision of "uninterrupted cryptographic protection of data between an originator and an intended recipient, including between an individual and himself or herself. It involves encrypting data by the originating party and keeping that data encrypted except by the intended recipient, where the means to access the data in unencrypted form is not given to any third party, including to any Internet service provider, application service provider or cloud service provider."

[1] The EAR, but not the ITAR, add "or other similarly effective cryptographic means" at the end of this provision.

The two agencies request comments concerning whether the new rules and encryption standards adequately address the export control issues for data storage and transmission. In particular, BIS requests comments regarding whether and how to reconcile certain differences between language proposed for the EAR and ITAR, including whether the illustrative standard proposed in the EAR rulemaking (*i.e.*, the addition of the phrase "or other similarly effective cryptographic means" to EAR § 734.18(a)(4)(iii)), should be added to the ITAR.

Complementing the exclusion for appropriately-encrypted technical data and software, other proposed new provisions of the EAR and ITAR define "export" and "reexport" to include releasing or otherwise transferring decryption keys, network access codes, passwords, software, or other information that would allow access to unencrypted controlled software or technology in "clear text"[2] to a foreign national, "regardless of whether such data has been or will be transferred." The wording of the decryption key paragraph is similar, but with some differences between the BIS and DDTC proposed rules, and the agencies request comments regarding which language more clearly describes the control.

A related proposed change is the addition of information to access secured technology or technical data (e.g., decryption keys, passwords, or network access codes) to the definitions of "technology" and "technical data." In addition, the rules would add new violation provisions providing that that any "release" of decryption keys or other access information that results in the unauthorized disclosure of the secured technical data, technology, or software will constitute a violation to the same extent as if the technical data, technology, or software itself had been exported.

These proposed changes are particularly relevant to users and providers of cloud storage services, although BIS specifically notes that "end to end" encryption is not used in all commercial situations utilizing the cloud. Under the current regulations, maintaining export-controlled data in cloud storage is challenging, because cloud storage providers may be unable to assure users that data will be kept in the United States; indeed, cost savings associated with cloud storage often depend in large part on the flexibility to store data across various U.S. and non-U.S. servers that are not necessarily identified in advance. Under the new rules, export-controlled data originating in the United States may be stored in one or more countries outside of the United States without licensing, provided the data is properly encrypted and not stored in countries subject to U.S. arms embargoes or in Russia. While the exclusion of embargoed countries and Russia means that these provisions would not authorize entirely unencumbered cloud storage, they would represent a major reduction in the restrictions on cloud storage of export-controlled data and software.

Revised Approach to Defense Services

The proposed redefinition of "defense service" in the ITAR follows proposed amendments to the definition introduced by DDTC on April 13, 2011 and May 24, 2013. Like the previous two proposed rules, this third proposed rule would narrow the ITAR's definition of "defense service,"

[2] The Supplementary Information accompanying the proposed rule to amend the EAR describes the term "clear text" as having "an industry standard definition, *e.g.*, information or software that is readable without any additional processing and is not encrypted."

permitting U.S. persons to engage without licensing in various types of conduct that currently require DDTC authorization.

The ITAR currently require U.S. persons to obtain authorization for the provision of defense services, which include furnishing assistance to foreign persons "in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles." ITAR § 120.9. The regulations also currently include as a type of defense service the export of technical data.

The proposed rule would eliminate the export of technical data from the defense services definition (such transfers still will be controlled as exports), focusing the definition solely on activities by U.S. persons that do not involve the provision of technical data.

Proposed revisions to the definition, to appear in ITAR §§ 120.9(a)(2) and (a)(3), would maintain the licensing requirement for U.S. persons assisting in the "development" of defense articles or the "integration" of defense articles with other items (whether commercial items or defense articles).

In other respects, however, the new definition is narrower than the existing definition. In particular, the proposed Section 120.9(a)(1) would limit the definition of defense service to assistance "in the production, assembly, testing, intermediate- or depot-level maintenance . . ., modification, demilitarization, destruction, or processing of a defense article . . .," to reach only assistance "by a U.S. person or foreign person in the United States, *who has knowledge of U.S.-origin technical data directly related to the defense article that is the subject of the assistance, prior to performing the service* . . . ." (Emphasis added.) Thus, these specific types of defense services are only covered if the person providing the services has knowledge of U.S.-origin ITAR technical data relating to the defense article at issue. The proposed rule accordingly focuses on what the U.S. person *knows* when providing the service, as opposed to what activity the U.S. person is undertaking or what technology the U.S. person uses to provide the service. This focus on knowledge is likely to present challenging issues both for prospective compliance planning and for retrospective assessment of compliance.

A note to the proposed rule provides that "U.S. persons abroad who only receive U.S.-origin technical data as a result of their activities on behalf of a foreign person are not included" among those U.S. persons deemed to be furnishing defense services due to their knowledge of U.S.-origin technical data. That provision may be useful for non-U.S. defense companies, as it would reduce the compliance burden of ensuring that those companies' U.S.- person employees abroad do not inadvertently provide unauthorized defense services to non-U.S. employees or entities. Nonetheless, this provision also may present challenging issues as companies seek to confirm how an employee came to learn certain information that they used when providing a service.

The proposed rule also identifies three other categories of defense services:

- "The furnishing of assistance" to a foreign person by a U.S. person "in the employment of a defense article, other than basic operation of a defense article authorized by the U.S. government for export to the same recipient;"

- "Participating in or directing combat operations for a foreign person . . ., except as a member of the regular military forces of a foreign nation by a U.S. person who has been drafted into such forces;" or
- The furnishing of assistance by a U.S. person to the government of China or another country subject to a U.S. arms embargo under ITAR § 126.1 "in the development, production, operation, installation, maintenance, repair, overhaul or refurbishing of a defense article or a part, component, accessory or attachments specially designed for a defense article."

These additional provisions ensure that some types of particularly sensitive conduct would remain regulated as defense services.

The overall thrust of the new proposed revisions to the definition is to reduce the number of activities considered as defense services that require authorization when provided to foreign parties. However, companies will need to give careful thought regarding how to ensure compliance with the requirements of Section 120.9(a)(1), if adopted as proposed. Moreover, given that the proposed rule would not materially modify the defense service definition as it relates to development activity (other than by excluding various administrative activities such as translation), companies will continue to be subject to significant compliance burdens with respect to services related to those activities.

Revisions of Other Key Definitions

In addition to the definition of "defense service" the rules propose revisions to other key export control terminology. Some notable proposed changes include:

Export, Reexport, and Deemed Export: The definitions of "export" and "reexport" would be revised to clarify the definitions and harmonize them between the EAR and ITAR. While the wording has changed, there are few significant substantive changes, with the exception of the changes discussed above to (1) exclude properly-encrypted data and software and (2) include the release or other transfer of decryption keys. Nonetheless, the proposed rules contain important confirmations of agency practice.

For instance, the proposed rules would codify the distinction between the treatment of nationality between the two agencies. The DDTC proposed rule provides that a release of technical data or software to a foreign person in the United States will be considered "a deemed export to *all* countries in which the foreign person has held citizenship or holds permanent residency," whereas the BIS proposed rule specifies that such a release "is a deemed export to the foreign national's *most recent* country of citizenship or permanent residency." (Emphasis added.) It is not clear from the ITAR proposed rule whether a release of technical data to a foreign person will be considered as an export to the foreign person's country of birth, which has been DDTC's approach.

The BIS proposed rule also codifies the "Deemed Reexport Guidance" BIS released on its website on October 31, 2013.

In addition, the DDTC proposed rule adds a new paragraph (a)(7) to the definition of "export" to address the public release of technical data (e.g., to the Internet). The provision clarifies that

releasing "technical data" to the Internet without government authorization constitutes a violation, even absent specific knowledge that a foreign person will read it.

Finally, the Supplementary Information to the proposed rules emphasizes that under the ITAR, merely providing physical access to unsecured technical data would be a controlled export, while providing such access to EAR technology will *not* be a controlled export unless done with "knowledge" that the provision of data will cause or permit the transfer of controlled technology to a foreign national.

Published and Public Domain: Relatedly, the agencies propose to update and broaden the definitions of "published" (EAR) and "public domain" (ITAR) to clarify that unclassified information and software are in the public domain (and thus not considered "technology" or "technical data" subject to export controls) "when they have been made available to the public without restrictions upon their further dissemination." Each definition clarifies that submission of a written manuscript or presentation to domestic or foreign co-authors, editors, or reviewers of journals, etc. with the intention to make the manuscript publicly available constitutes releasing the manuscript to the public domain. Pursuant to the proposed ITAR definitions, ITAR-controlled technical data is not considered to be in the public domain if it is publicly released without authorization (i.e., without authorization from DDTC, the Department of Defense's Office of Security Review, or another U.S. government entity or official authorized to approve the release). Relatedly, the proposed rule prohibits exporting, reexporting, or "otherwise mak[ing] available to the public technical data or software if" the person making it so available "has knowledge that the technical data or software was made publicly available without . . . authorization."

Release: DDTC proposes to define the term "release," which is used in the definitions of "export" and "reexport," to harmonize with the EAR, which uses the term to cover activities that disclose information to non-U.S. persons. In both proposed rules, the definition of "release" would specifically include oral or written exchanges of technical data with a non-U.S. person and permitting a non-U.S. person to inspect a defense article in a way that reveals technical data. Notably, the Supplementary Information to the proposed rules emphasizes that visual inspections must *actually* reveal controlled technology or source code to constitute a release. As BIS states in its proposed rule, "[M]erely seeing equipment does not necessarily mean that the seer is able to glean any technology from it, and, in any event, not all visible information pertaining to equipment is necessarily 'technology' subject to the EAR."

In addition, the BIS rule amends existing BIS practice by providing that the "application by U.S. persons of 'technology' or 'software' to situations abroad using personal knowledge or technical experience acquired in the United States" is only treated as a release to the extent that the "application reveals to a foreign national 'technology' or 'source code' subject to the EAR." This changes the existing BIS rule by adding the limitation that the restriction only applies if the U.S. person reveals controlled technology or source code to a foreign national.

Technology and Technical Data: The definitions of "technology" and "technical data" would be harmonized in the two rules and based on the Wassenaar Arrangement definition of "technology." The DDTC rule also proposes related new definitions of "development" and "production" technology as relevant to "technical data" and "defense services"; these definitions are consistent with existing EAR definitions. In addition, DDTC would remove software from the definition of "technical data" and include it as a type of "defense article." With respect to the

Commerce proposed rule, BIS clarifies and confirms in the preamble text that information that is not "technology" as defined by the EAR is not subject to the EAR.

Peculiarly Responsible and Required: BIS proposes a definition of "peculiarly responsible" and two notes to clarify its existing definition of "required," and DDTC proposes to adopt a definition of "required." The definitions of "peculiarly responsible" and "required" each establish a test for determining if an item or information "is peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions of" the controlled item. These definitions use the same catch-and-release concept used in the definition of "specially designed" in the EAR and ITAR. In general, the proposed definitions would "catch" information as "technology" or "technical data" if it is "'peculiarly responsible' for achieving or exceeding the controlled performance levels, characteristics or functions" of a controlled item, and then exclude or release items that meet certain specified criteria.

Authorization for "Defense Services" Provided by U.S. Persons Employed by Non-U.S. Persons

As noted above, DDTC also has published a separate proposed rule that addresses "defense services" provided by natural U.S. persons working for non-U.S. companies overseas. In the past, DDTC policy toward registration and licensing of natural U.S. persons working for non-U.S. companies overseas has been less than clear. Currently, such defense services in principle would require the U.S. employee to register with DDTC and obtain a Technical Assistance Agreement ("TAA") between the U.S. person employee and his or her employer; however, industry practice on this has varied considerably.

DDTC attempted to clarify its policy in April 2013, by adding text to DDTC's "Agreements Guidelines," clarifying that defense services provided by a U.S. person employed abroad would not be authorized by a TAA to which the employee's non-U.S. employer was a signatory, unless the U.S. person employee also was a signatory. To obtain authorization for a U.S. person employed abroad to provide defense services, DDTC advised that the U.S. person could register with DDTC and be a signatory to one or more TAAs that covered the services the person would perform. This text was controversial with industry, which expressed concern that it would impose an excessive burden on non-U.S. operations. As a result, the text was withdrawn in October 2013.

In the new proposed rule, DDTC clarifies that "any U.S. person who engages in the business of furnishing defense services wherever located is required to register with DDTC." ITAR § 122.1. Accordingly, U.S. persons (including dual nationals of the United States and another country) who provide defense services to or on behalf of their employer and who are (i) "regular employees" of a non-U.S. company, or (ii) employed by a non-U.S. person as independent contractors must be registered with DDTC.

The new rule also provides that any natural U.S. person directly employed by a DDTC registrant, "or by a person listed on the registration as a subsidiary or affiliate of a DDTC-registered U.S. person, is deemed to be registered." Thus, the registration requirements of many U.S. persons should be covered by their employer's registration or the registration held by their employer's parent company. However, subsidiaries and affiliates (including non-U.S. subsidiaries and affiliates) may only be added to the registration of a DDTC-registered U.S. person if they are "controlled" by the registrant. Thus, non-U.S. employers who are not

controlled by their registered affiliates, or who do not have registered U.S. affiliates, may not be able to benefit from this provision.

The proposed rule would permit a DDTC registrant to "establish a control relationship with another entity via written agreement such that the entity then becomes an affiliate" that may be included on the DDTC registrant's registration, "subject to DDTC's disallowance." DDTC's Supplementary Information states that this is intended "to clarify that under specified circumstances, minority owners of a firm may list that company [in which they hold a minority stake] under their registration." However, the scope of this provision is unclear -- for example, with respect to whether the provision applies to unrelated companies or a foreign parent of a DDTC-registered subsidiary, if a registrant is willing to establish a written "control relationship" with the other entity.

In addition to registering, U.S. person employees of non-U.S. persons also would need to obtain authorization for their defense services if the proposed rule is adopted. Under the proposed rule, natural U.S. persons would be able to obtain DDTC approval for their defense services in a number of ways.

- One way of obtaining authorization is through a DSP-5 export license.
- An agreement between a foreign employer listed on the registration of a U.S. person and the U.S. registrant also could be used, "provided that the registered U.S. person accepts responsibility for, and demonstrates ability to ensure, the natural U.S. person's compliance with the provisions of [the ITAR]." It is unclear exactly what form this acceptance of responsibility should take. Further, there may be practical limitations on the ability of a U.S. affiliate to monitor and ensure the compliance of natural U.S. persons employed by non-U.S. persons, particularly if those natural U.S. persons are located overseas.
- An exemption also is available to non-U.S. persons whose employer is located within a North Atlantic Treaty Organization or European Union country, Australia, Japan, New Zealand, and/or Switzerland. The exemption is subject to certain conditions, including that the defense services be provided only in these countries and only to end users in these countries, and is premised on compliance with recordkeeping and registration requirements.

Also, no license would be required for defense services provided in support of an active foreign military sales contract that are identified in an executed Letter of Offer and Acceptance, provided that conditions similar to those required for the exemption above are met.

* * *

We are well-positioned to advise clients regarding the impact that these proposed rules would have on their operations and to assist companies in submitting comments to BIS and DDTC on these or other issues. As noted, comments on the proposed definitions rules will be accepted until August 3, 2015. Comments on the rule clarifying requirements for defense services provided by natural U.S. persons working for non-U.S. companies will be accepted until July 27, 2015.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our international trade controls practice group:

Peter Flanagan	+1 202 662 5163	pflanagan@cov.com
Corinne Goldstein	+1 202 662 5534	cgoldstein@cov.com
Peter Lichtenbaum	+1 202 662 5557	plichtenbaum@cov.com
Kim Strosnider	+1 202 662 5816	kstrosnider@cov.com
David Addis	+1 202 662 5182	daddis@cov.com
Damara Chambers	+1 202 662 5279	dchambers@cov.com
Eric Sandberg-Zakian	+1 202 662 5603	esandbergzakian@cov.com