International Trade

September 1, 2016

Redefining U.S. Export Controls: Takeaways from Key Changes Effective September 1st

By Nancy A. Fischer, Stephan E. Becker, Aaron R. Hutman, Benjamin J. Cote, Matthew R. Rabinowitz and Moushami P. Joshi

On September 1, 2016 new rules previously published by the U.S. Department of Commerce, Bureau of Industry and Security (BIS)[1] and the U.S. Department of State, Directorate of Defense Trade Controls (DDTC)[2] will become effective. These rule changes will revise key definitions in both the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR). Following is an overview of takeaways from the final rules and how they may impact companies moving forward.

Takeaway 1 – EAR-controlled transmissions through the Cloud generally will no longer be considered an "export" where encrypted end-to-end, but a similar change has not yet occurred in the ITAR.

Building off of rules proposed in June 2015, the final rules stand to positively affect cloud services and other encrypted technology and software. For example, companies can store EAR-controlled software and technology on cloud servers based in most countries without "exporting" the data to those countries.

BIS redefined "export , reexport, or transfers" to *exclude* sending, taking, or storing technology or software so long as it is:

1. Unclassified[3]

2. Secured using "end-to-end" encryption; that is, the data must be encrypted *before* crossing a national boundary and stay encrypted while being transmitted from one security boundary to another, so long as no third party has the ability to access the data in clear text;[4]

[1] Department of Commerce, Revisions to Definitions in the Export Administration Regulations, 81 F.R. 35586 (June 3, 2016) ("BIS Rule").

[2] Department of State, International Traffic in Arms: Revisions to Definition of Export and Related Definitions, 81 F.R. 35611 (June 3, 2016) ("DDTC Rule").

[3] "Unclassified" means that the software or technology is not classified in accordance with E.O. 13526. BIS Frequently Asked Questions (FAQs).

3. The encryption is at least as effective as that compliant with Federal Information Processing Standards Publication (FIPS) 140-2 supplemented by procedures and controls according to National Institute for Standard and Technology publications; and

4. Not intentionally stored in a D:5 arms embargo country or in Russia.[5]

Importantly, this carve-out does not currently apply in the ITAR context. DDTC has stated that it will address analogous controls on encrypted technical data in a separate rulemaking. As a result, companies with both ITAR and EAR items should not assume they can apply the same compliance procedures for cloud services in both contexts.

Takeaway 2 – Alternative security may be used for encrypted transmissions, but the burden is on the sender to ensure effectiveness.

With respect to the new EAR rule for transmissions through the Cloud, exporters can use third-party or internally developed cryptography that is not NIST-certified, because the final rule allows for encryption "at least as effective" as FIPS 140-2. On the other hand, BIS's FAQs make clear that the onus is on companies to ensure that whatever security means they use are effective in the context the company operates.[6] Transmissions lacking adequate security could therefore be treated as exports, with the associated export liability.

Takeaway 3 – An export requires a "release" that actually reveals technology or technical data to a foreign person.

Companies whose procedures allow "theoretical access" by foreign persons to EAR-controlled items requiring authorization are not necessarily in violation. The BIS final rule clarifies that a foreign person's having *theoretical or potential access to technology or software* is similarly not a "release" because such access, by definition, does not reveal technology or software.[7] In other words, under the EAR the fact that persons have access to a computer system in general does not automatically mean that they will be deemed to have received controlled data stored in a file in the computer system.

In addition, inspection (visual, aural or tactile) of an item must *actually reveal* technology or source code subject to the EAR to constitute a "release." Therefore, merely seeing an item briefly is not necessarily sufficient to constitute a release of the technology required to develop or produce it.[8]

Separately, DDTC stated in its final rule that to constitute a "release" under the ITAR, information about the defense article must be technical data and not simply attributes, such as size or weight.[9]

[4] Ability to access the technology or software in encrypted form satisfying the encryption in 734.18(a)(5) is not a release. EAR § 734.18(c) (effective Sept. 1, 2016).

[5] EAR § 734.18(a)(5) (effective Sept. 1, 2016).

[6] BIS FAQs, Q.4.

[7] BIS Rule, 81 F.R. at 35592.

[8] BIS Rule, 81 F.R. at 35592.

[9] DDTC Rule, 81 F.R. at 35614.

Takeaway 4 – Causing a "release" using a password is treated like an export or reexport.

Under the new BIS rule, a person who uses a password to access a technology database, or who hacks into the database, to transfer technology to himself or someone else is the one who caused the release of technology, rather than the person who first placed the technology in the database. The rule states that causing the "release" of technology or software, through *use* of "access information" or otherwise, to one's self or another person, is treated the same as an export or reexport to that person.[10] Access information is information that allows access to encrypted technology or software in an unencrypted form. Examples include decryption keys, network access codes, and passwords.

In contrast, *providing* access information by itself to another would require authorization only to the extent it is done with "knowledge" (e.g., "awareness of a high probability") that the transfer would result in a "release" without a required authorization.[11] This reflects BIS's intent not to control "access information" as a distinct item.

For its part, DDTC indicated that while providing physical access is not an "export," any release of technical data to a foreign person is an export. If a foreign person views or accesses technical data as a result of being provided physical access, then an "export" has occurred and the person who provided the foreign person with physical access to the technical data is an exporter responsible for ITAR compliance.[12]

Takeaway 5 – When a product is modified, technology *common* to both original and modified versions is distinct from *additional* technology used to modify the original product.

The BIS final rule also addresses situations where companies struggle to classify technology associated with multiple variations of a product by describing technology for modification of a design.[13] In its guidance, BIS describes a scenario where a company manufactures a switch for a civil aircraft, with the switch being controlled under ECCN 9A991.d. The company later modifies the switch for use in a military aircraft, resulting in the item being controlled under ECCN 9A610.x. In this case, technology *common to both* switches is controlled under ECCN 9E991, while the *additional or different technology* to make the switch a military switch is controlled under ECCN 9E610 as production or development technology for the 9A610.x military switch.[14]

Takeaway 6 – Different ITAR and EAR standards for deemed exports remain.

It is long-standing BIS policy that when technology is released to a foreign national, the export is deemed to occur to that person's most recent country of citizenship or permanent residency.[15] The BIS final rule codifies this policy within the definition of "export."[16]

In contrast, DDTC has maintained that disclosing technical data to a foreign person in the U.S. is deemed to be an "export" to all countries in which the foreign person holds or has held citizenship or holds permanent residency. In its final rule, DDTC states that it will continue this policy.

[10] EAR §734.15(b) (effective Sept. 1, 2016).
[11] EAR §734.19 (effective Sept. 1, 2016). The "release" provision at EAR §734.15(b) contains no such knowledge requirement.
[12] DDTC Rule, 81 F.R. at 35613.
[13] EAR §772.1 ("technology") (effective Sept. 1, 2016).
[14] BIS Rule, 81 F.R. at 35597.
[15] ITAR §120.17(b) (effective Sept. 1, 2016).
[16] EAR §734.13(b) (effective Sept. 1, 2016).

If you have any questions about the content of this Alert, please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Nancy A. Fischer (bio)
Washington, DC
+1.202.663.8965
nancy.fischer@pillsburylaw.com

Stephan E. Becker (bio)
Washington, DC
+1.202.663.8277
stephan.becker@pillsburylaw.com

Aaron R. Hutman (bio)
Washington, DC
+1.202.663.8341
aaron.hutman@pillsburylaw.com

Benjamin J. Cote (bio)
Washington, DC
+1.202.663.8305
benjamin.cote@pillsburylaw.com

Matthew R. Rabinowitz (bio)
Washington, DC
+1.202.663.8623
matthew.rabinowitz@pillsburylaw.com

Moushami P. Joshi (bio)
Washington, DC
+1.202.663.8021
moushami.joshi@pillsburylaw.com