DDTC aligns technical data export rules with BIS rules, simplifying technical data controls

January 1, 2020

Late last month, the Directorate of Defense Trade Controls issued a long-awaited interim final rule regarding what qualifies as the export, re-export, or transfer of technical data (a "controlled event") under the International Traffic in Arms Regulations ("ITAR"). Specifically, in 2016, the Bureau of Industry and Security ("BIS") issued a final rule clarifying that the transmission of technology outside of the U.S. using end-to-end encryption did not qualify as a controlled movement, provided that the technology is encrypted up to a specified standard. DDTC did not adopt an equivalent provision in its version of an overlapping final rule, creating significant compliance and logistical considerations for companies falling under the jurisdiction of both entities, especially those entities for which it was impractical to consolidate all IT infrastructure within the U.S.

In the interim final rule, DDTC is largely aligning its rules regarding "controlled events" with BIS's rules, making DDTC's treatment of technical data much more permissive than it is currently. Provided that all of the following are satisfied, sending/storing technical data will not qualify as an export: 1) the technical data is unclassified; 2) it is secured using end-to-end encryption; 3) it is secured using cryptographic modules compliant with FIPS 140-2 or equivalent standard; 4) it is not intentionally sent to a person or stored in a proscribed country (i.e., listed in ITAR 126.1) or the Russian Federation; 5) it is not sent from a proscribed country. These amendments are included in a new section of the ITAR, located at 22 C.F.R. 120.54.

Although this alignment does simplify companies' responsibilities regarding the storage and transmission of technical data, compliance concerns remain that must be mitigated. First, if the technical data is decrypted by someone other than the sender, a U.S. person in the U.S., or a person otherwise authorized to receive the technical data, then the technical data is not secured using end-to-end encryption and the original transmission will be deemed a controlled event. Further, DDTC declined to create a safe harbor under which companies would only have to seek contractual assurance from cloud providers that technical data would not be stored in a 126.1 country or the Russian Federation to satisfy the ITAR provision. Instead, DDTC specifies in the rule that it will continue to evaluate potential violations related to technical data release under a totality of the circumstances framework.

As an interim final rule, DDTC is accepting public comments until January 27, 2020. The rule becomes effective on March 25, 2020.