Proposed Export Rules for Technology and Cloud Computing

— hugheshubbard.com — eALERT

State and Commerce Proposed Rules:
Overhaul of Export Controls on Technical Data and Cloud Computing

On June 3, the U.S. Departments of State and Commerce published proposed rules that would change or clarify definitions of several key terms in State's International Traffic in Arms Regulations ("ITAR") and Commerce's Export Administration Regulations ("EAR") and that would change the way the Departments regulate data storage and transmission, including cloud services. The proposed rules are part of the broader Export Control Reform Initiative, which aims to update export controls and reduce regulatory burdens on exporters. These are proposed rules only; both agencies will accept comments on the proposals up to August 3, 2015. The following is a brief summary of some of the key provisions in the proposals.

- The proposed rulemakings focus on the agencies' interpretations and regulation of the export of technical data, and they largely serve to harmonize the usage of identical terms between the ITAR and EAR to avoid confusion. The changes are especially relevant to companies engaging in the development, storage, and transmission of export-controlled technical data, including cloud computing. They also will be relevant to any company that uses third-party cloud service providers for the storage of their export-controlled technology.

- Perhaps the most significant proposal would exclude the transmission and storage of encrypted technical data and software from ITAR and EAR licensing requirements. Both agencies recognize that, for example, cloud storage of data could involve servers located in foreign countries. Currently, providing even unintended access to such data to a foreign person would constitute an export of controlled technical data. With this change, the transmission and storage of data in foreign locations en route to a recipient would not be considered an export, if the data remains encrypted while in transit from the United States to its authorized destination through end-to-end encryption; the two agencies have slightly different standards for what would qualify for end-to-end encryption. If data transmission meets this requirement, its passage through or storage on non-U.S. servers would be allowed, so long as the server is not in a restricted country or in the Russian Federation. The same change would allow companies to store encrypted data on servers in an acceptable country, even if non-U.S. nationals could have access to the server. If adopted, this proposal would significantly reduce administrative burdens on companies reliant on access to sensitive data.

- The proposals also would permit foreign persons already authorized to receive technical data while in the U.S. to receive that same data while abroad during the course of their employment. If adopted, this would streamline current logistical difficulties with ensuring continued access to necessary data.

- Both Departments are proposing language that would make unauthorized provision of information that would grant *access* to controlled technical data, such as providing decryption keys or passwords, an export control violation. However, under certain circumstances, provision of *encrypted* technical data would not qualify as an export under the proposals.

- The State proposal would reduce the scope of ITAR-controlled technical data by making the carve out for information available in the "public domain" less rigid and more responsive to changes in technology, particularly the electronic dissemination of information.

- The State proposal would redefine the term "defense services" under the ITAR. Among other things, the simple export of ITAR-controlled technical data would no longer be a defense service, but would be regulated as a straight export. If the exporter would need to modify or otherwise work with the exported data, however, that would still be a technical service requiring a Technical Assistance Agreement.

- The rulemakings would define what is meant by "peculiarly responsible" where that term is used as part of a technical data export classification.

- The changes would clarify the requirement that, prior to disseminating ITAR-controlled technical data into the public domain, there is an absolute requirement to receive authorization from the government. This codifies existing practice. However, State has clarified that the dissemination of ITAR-controlled technical data *already in* the public domain is not a violation, unless the party had actual knowledge that the data is not properly in the public domain.

- The Commerce Department is proposing to codify its 2013 published policy, which corresponds to existing provisions of the ITAR, to exclude from re-export controls transfers of technology to third-country nationals working outside the United States, if certain criteria are met. The Commerce Department also would include a definition of "substantive contacts" with the same meaning as it already has under the ITAR, when evaluating the third-country national's ties to his or her country of origin.

- Both Departments are accepting comments until August 3, 2015, and have specifically requested industry comments regarding: 1) how adequately the proposed regulations address the technical aspects of data transmission and storage; 2) whether the proposed regulations mitigate unintended or unauthorized access to transmitted or stored data; 3) whether the proposed regulations would impose an undue financial or compliance burden.

For further information, please contact:

F. Amanda DeBusk, *Partner*
+1 (202) 721-4790
amanda.debusk@hugheshubbard.com

Melissa Duffy, *Partner*
+1 (202) 721-4689
melissa.duffy@hugheshubbard.com

Alan Kashdan, *Counsel*
+1 (202) 721-4630
alan.kashdan@hugheshubbard.com

Hughes Hubbard
Critical matters. Critical thinking.®

International Trade and Customs Practice Group

June 2015

Hughes Hubbard & Reed LLP
One Battery Park Plaza | New York, New York 10004-1482 | +1 212-837-6000