International Trade

June 23, 2015

Proposed Change to Export Controls Would Allow Use of the Cloud for Encrypted Data

By Christopher R. Wall and Sanjay J. Mullick

On June 3, 2015 the State Department's Directorate of Defense Trade Controls (DDTC) and the Commerce Department's Bureau of Industry and Security (BIS) published proposed regulations which would change the definition of the term "export" in each agency's regulations to allow cloud storage of information in servers located in foreign countries if the information is appropriately encrypted.[1] These changes, if ultimately adopted, would substantially alleviate concerns that companies seeking to take advantage of the efficiencies of cloud computing could run afoul of export controls. However, it would still be important for cloud users and cloud storage providers to ensure that appropriate encryption is being used.

End-to End Encryption

The key element of the proposal is that the technical data, technology or software be encrypted by the originator at the sending point and remain unreadable at every point in transit or in storage without interruption until decrypted by the intended recipient or retrieved by the sender ("end-to-end" encryption). This means that no third party, including any Internet service provider or cloud storage provider, could have means to access the data in unencrypted form ("clear text"). The agencies' view is that if no foreign persons can gain access to such data, then it is not useful to unauthorized parties and poses no threat to national security, and accordingly there is not an "actual" transmission.

Under the new definitions, providing physical access or the release or other transfer of the means of access to encrypted data, such as cryptographic keys, passwords and network access codes, would be

[1] See 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. 31525 (June 3, 2015) and Revisions to Definitions in the Export Administration Regulations, 80 Fed. Reg. 31505 (June 3, 2015).

considered an export. The password or code that allows access to the data would be treated as having the same classification and control status as the corresponding related technical data, technology or software. The agencies' rationale is that providing the means to decrypt or otherwise access technical data should be treated as if the data itself were released. For enforcement purposes, such an unauthorized release would constitute a violation to the same extent as one in connection with the export, reexport, or transfer (in-country) of the technical data, technology or software itself.

The proposal to exclude from the definition of "export" appropriately encrypted technical data, technology or software sent to or taken from the cloud would not extend to servers located in Russia or in countries designated under section 126.1 of the International Traffic in Arms Regulations (ITAR) or in Country Group D:5 of the Export Administration Regulations (EAR), such as China.

Different Approaches by State and Commerce

Although DDTC and BIS follow similar approaches, there are some differences in how their regulations would apply. DDTC, for example, would specifically require use of encryption modules certified by the U.S. National Institute for Standards and Technology (NIST) under the Federal Information Processing Standard 140-2 (FIPS 140-2), which is a cryptographic standard used for Federal Government procurement. DDTC would also require that such certified encryption modules be supplemented by appropriate software implementation, cryptographic key management and other procedures or controls that are in accordance with guidance provided in current NIST publications. BIS would permit use of alternative encryption approaches provided they are "similarly effective," but BIS emphasizes that "the exporter is responsible for ensuring they work."

DDTC proposes to treat providing access to unsecured technical data as a controlled event, regardless of whether that data has been or will be transferred (i.e., regardless of whether foreign persons were intended to access or have actually accessed the data). On the other hand, BIS will only consider providing access to unsecured technology to be a controlled event if it is done with "knowledge" that doing so will cause or permit the transfer of controlled technology or software to a foreign national.

New Compliance Concerns

The new definition of "export" in the context of cloud computing will shift the compliance emphasis from identifying the location of servers to ensuring that appropriate encryption safeguards are in place.

Users of the cloud currently must be concerned about whether their data might be sent for storage in a server anywhere outside the United States to avoid unintended exports. If the proposed rules are adopted, this concern will not be as significant, except to the extent that the regulations would continue to make ineligible the location of servers in embargoed countries as well as Russia and China. Cloud users, however, would have to make sure they are implementing appropriate encryption or otherwise be assured of the type of encryption implemented by third party service providers. Also, companies may need to implement specialized security protocols for screening the nationality of employees that have access to encrypted data or keys.

Under prior BIS advisory opinions, compliance responsibility largely rested with the entity whose data was stored in the cloud. Under the new definitions, cloud storage providers will also have responsibility for compliance. They may alter their business models to market services that will be viewed as compliant by offering encryption modules that will satisfy the new regulatory requirements

This is the most significant step taken by the U.S. government to address export control issues in the context of cloud computing and the first step taken by regulation rather than by advisory opinion. The agencies are seeking comments to the proposed rules by August 3, 2015 on issues including whether the encryption standards adequately address the technical aspects of data transmission and storage, and whether they mitigate unintended or unauthorized access to transmitted or stored data.

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

Christopher R. Wall (bio)
Washington, DC
+1.202.663.9250
cwall@pillsburylaw.com

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

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

Sanjay J. Mullick (bio)
Washington, DC
+1.202.663.8786
sanjay.mullick@pillsburylaw.com

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

Matthew Oresman (bio)
London
+44.20.7847.9516
matthew.oresman@pillsburylaw.com

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

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

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.