International Trade | Public Policy

Corporate & Securities – Technology | Privacy, Data Security & Information Use

May 28, 2015

Strict Controls Proposed on the Export of Cybersecurity Items

By Brian Finch and Sanjay Mullick

On May 20, 2015, the Commerce Department Bureau of Industry and Security (BIS) proposed to establish controls on the export of cybersecurity items. These items would be classified under new Export Control Classification Numbers (ECCNs) in Categories 4 and 5 of the Export Administration Regulations (EAR) that would be subject to Regional Stability (RS) controls, which require licenses for all countries except Canada and generally are not eligible for license exceptions. If the proposed rules are implemented, strict licensing requirements would be imposed on the export of these items, even those that companies may themselves legitimately seek to obtain to test how vulnerable their networks may be to cyberattacks.

Under the proposed rule, BIS considers the following to be cybersecurity items:

1. Systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software;

2. Software specially designed or modified for the development or production of such systems, equipment or components;

3. Software specially designed for the generation, operation or delivery of, or communication with, intrusion software;

4. Technology required for the development of intrusion software; and

5. Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor.

The term “intrusion software” is defined, e.g., as software specially designed or modified to avoid detection by monitoring tools, or to defeat protective countermeasures. “Monitoring tools” are defined as software or hardware tools that monitor system behaviors processes running on a device, and “protective countermeasures” are defined as techniques designed to ensure the safe execution of code.

In proposing these changes, BIS is seeking to implement agreements made in December 2013 by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Technologies (Wassenaar Arrangement). The Wassenaar Arrangement is a group of 41 countries that seek to promote harmonization of export controls by adopting similar lists of controlled items. Once changes are agreed to, participants such as the United States are expected to follow through with making such changes to their own national export control lists.

BIS acknowledges that the items it proposes to regulate under the new cybersecurity controls “include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices.” Currently, certain of these items are controlled for export as encryption items because of their information security functionality. However, under License Exception ENC, most encryption items can be freely exported except to embargoed countries after registering with BIS, filing a classification request and undergoing a 30-day waiting period. The principal exception is a category of certain “restricted products,” e.g., network infrastructure items, which require a license if exported to foreign government customers in countries outside the list contained at Supplement No. 3 to Part 740 of the EAR.

Under the proposed rule, if cybersecurity items implement encryption, exporters will still have to comply with License Exception ENC’s requirements. But rather than resulting in export authorization, fulfilling these steps will simply be prerequisites to applying for an export license, which will be required for all countries except Canada. Exporters who believe their items are subject to the encryption controls should exercise caution, to avoid a situation in which they export and then learn after the fact that BIS actually believes the items are subject to the new cybersecurity controls.

Also, License Exception ENC permits the export of encryption items to subsidiaries of U.S. companies without prior authorization. However, the proposed cybersecurity controls would still require an export license in those instances. This restriction will potentially complicate deployment of cybersecurity items by U.S.-based multinational corporations even for protective purposes within the corporate family.

Companies across the globe, particularly U.S.-based companies operating overseas, are constantly under cyber-attack. It is vital that they have the best cybersecurity system possible in place, which requires regular and rigorous testing of those defenses. It may prove difficult to strike the right balance between preventing cybersecurity items from falling into the wrong hands to conduct cyberattacks and allowing companies legitimate access to them so they can test their cyber defenses.

Comments to the proposed rule are due by July 20, 2015. In particular, BIS is seeking comments, e.g., on to what degree the proposed rule would increase the number of license applications companies would have to make and whether it would have negative effects on a company’s ability to protect its own networks. Nonetheless, as BIS is required to implement the multilateral Wassenaar Arrangement agreement, there may be limited opportunity to make significant changes to the proposed rules before they go into effect.

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.

Brian Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

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