Uncertain Fate of Cybersecurity Export Rule Following Congressional Inquiry

hugheshubbard.com

eALERT

The U.S. government is back to the drawing board to implement export controls on intrusion software tools and Internet Protocol ("IP") network communications surveillance systems. Following a landslide of industry comments, culminating in a Congressional hearing this past week, it is clear that the government is far from resolving this issue. What is apparent is that the Administration plans to keep working at it, and the active engagement of cybersecurity companies in this process will be critical to getting it right.

In December 2013, the Administration agreed to amend the Wassenaar Arrangement (an agreement among 41 countries to set export control thresholds for munitions and dual-use items), which would require the U.S. to adopt new export controls on certain cybersecurity items. The purpose of the amendment would be to keep such items, including cyber intrusion and surveillance technologies, from being exported to foreign governments for use in human rights abuses against their populations. This export control effort has been controversial, due to the difficulty in implementing a control that does not at the same time restrict the legitimate development and exchange of these tools for positive cybersecurity purposes.

In May 2015, the Department of Commerce, Bureau of Industry and Security ("BIS") requested comments on a proposed rule ("Proposed Rule") to implement the Arrangement's cybersecurity export controls. *See* 80 Fed. Reg. 28853 (May 20, 2015), *available at* https://federalregister.gov/a/2015-11642. Under the Proposed Rule, a license would be required to export "cybersecurity items" to all countries but Canada. Cybersecurity items would be defined to include systems, equipment, components, and software designed to make, operate, deliver, or communicate with "intrusion software" (i.e., software designed to avoid detection or defeat protective countermeasures that is cable of extracting data or information from a computer, or modifying the standard execution party of a program to allow the execution path of externally provided instructions), as well as IP network communications surveillance systems or equipment. *See* 80 Fed. Reg. at 28854. It would also include technology for the development of intrusion software, including "proprietary research on the vulnerabilities and exploitation of computers and network-capable devices." *Id*.

U.S. industry overwhelmingly responded with 264 comments that identified many unintended negative consequences if the rule were finalized. Commenters in particular feared that the Proposed Rule's broad definitions would require licenses for necessary sharing of information regarding security breaches and vulnerabilities. The majority view was that the licensing burden would be overwhelming for both the government and for the tech sector, and it would significantly

delay companies' effective responses to cyber-attacks. Commenters said that licensing requirements would impair the sharing of cybersecurity information among foreign nationals and affiliates within companies, as well as the receipt of vulnerability reports from private individuals through "bug bounty" programs. BIS has not reissued the proposed rule or published further guidance on its plans since the comment period closed on July 20, 2015.

On January 12, 2016, the U.S. House of Representatives held a joint[1] hearing to solicit testimony regarding the negotiations behind the 2013 Wassenaar Arrangement amendment, the Administration's process for developing the proposed rule, and to discuss future steps for controlling cybersecurity technologies. (A recording of the hearing and related written materials is available at https://oversight.house.gov/hearing/wassenaar-cybersecurity-and-export-control/.) The testimony came from witnesses representing government agencies (Departments of State, Commerce, and Homeland Security) as well as representatives from industry stakeholders (Microsoft Corp., Symantec, VMware, Inc., and the Information Technology Industry Council).

Comments at the Hearing

Industry testimony raised concerns about whether the Proposed Rule could be revised to address the issues raised in the public comments without renegotiating the 2013 amendment. The Administration panelists declined to commit to renegotiating the Wassenaar Arrangement cybersecurity provisions at this time, but they indicated that they intend to seek out and be responsive to industry concerns. The Administration made clear that its next step will not involve issuance of a final rule, which implies that another proposed rule accompanied by solicitation of industry comments may be forthcoming.

Key points made at the hearing include:

- The government witnesses explained that the Administration had followed its normal annual Wassenaar process and formulated the proposal with input through its technical advisory committee process, which did not, at that time, identify any concerns. The Administration also took the unusual step in this case of submitting a proposed rule for public comment, rather than just immediately publishing a final rule with the Wassenaar changes. The Administration panelists indicated their intention to keep the cybersecurity sector closely engaged with this process.

- The industry witnesses, and many of the Representatives on the Committee, raised concerns that renegotiation of the 2013 amendment would be necessary. The government panelists, however, stressed that renegotiation would be diplomatically difficult at this time because 31 of 41 Wassenaar parties already have implemented the amendment. They further stated that it this time the Administration had made no decision on implementation of the amendment, other than that it would not yet issue a final rule.

- Industry witnesses pointed out that, because a majority of the world's cybersecurity firms are located in the U.S., the U.S. disproportionately bears the burden of the Arrangement's proposed cybersecurity controls. Further, certain countries with large technology industries (e.g., Brazil, India, China) are not parties to the Arrangement, and thus not subject to the proposed controls.

- Industry witnesses and some Representatives on the Committee also suggested that alternatives to the Wassenaar Arrangement for controlling exports of cybersecurity technologies could be explored, such as existing criminal legislation or economic sanctions targeting the malicious use of cyber intrusion tools.

What to Expect Next

The hearing underscored that, while the Administration has decided not to proceed yet with a final rule implementing the 2013 Wassenaar Arrangement cybersecurity controls, next steps are still up for discussion. While it is unclear at this time whether the Administration will issue a revised proposed rule and solicit comments, attempt to renegotiate the 2013 amendment at the Wassenaar multilateral level, or take another course of action, the government witnesses at the hearing affirmed that the Administration intends to be responsive to industry feedback going forward. U.S. companies that could be affected by the rule should be alert for ongoing developments in the coming months, and be prepared to respond swiftly to any requests for comments or feedback from the Administration.

[1]The hearing was held by the Oversight Subcommittee on Information Technology and Security and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.

For more 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

Tyler Grove, *Associate*
+1 (202) 721-4625
tyler.grove@hugheshubbard.com

International Trade and Customs
Digital Trade: Cybersecurity, Encryption and Cloud Services
January 2016

Hughes Hubbard & Reed LLP