WILMERHALE

Support Continues to Build for New Export Controls on Cyber Monitoring Technologies

2013-12-13

Amid growing worldwide concern about the security of commercial and government computer networks, the leading multilateral export control organization has moved toward new export controls for advanced computer network hardware, software and technologies that can be used to exploit cybersecurity vulnerabilities. Last week, at meetings in Vienna, Austria, the international consortium of 41 arms-exporting countries known as the "Wassenaar Arrangement" agreed that export controls should be established for "Internet Protocol (IP) network surveillance systems or equipment, which, under certain conditions, may be detrimental to international and regional security and stability."[1]

The United States already imposes export controls for equipment, software and technologies for mobile telecommunications interception or jamming equipment, surreptitious interception of communications, and encryption items that provide penetration capabilities for attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks. This new development signals an emerging consensus among export regulators that such existing controls may no longer be adequate.

Agreements under the Wassenaar Arrangement must be implemented separately by each member state. Although the precise impact of the agreement reached in Vienna on US exporters is not yet clear, vigilance is in order. New export controls or a tightening of existing controls could have a substantial impact on US companies in the future.

Independent of the Wassenaar decision, the United States Congress is separately considering new export controls associated with cybersecurity technologies and offensive cyber "weapons." Both the House and Senate versions of the 2014 National Defense Authorization Act (NDAA) would require the President to study ways to contain the proliferation of "cyber weapons." Section 940 of the House-passed version of the 2014 NDAA, which cleared the House on December 12, 2013, requires the President to:

> establish an interagency process to provide for the establishment of an integrated policy to control the proliferation of cyber weapons through unilateral and cooperative

> law enforcement activities, financial means, diplomatic engagement, and such other means as the President considers appropriate.[2]

The bill also requires the President to include private industry representatives in the process "to the extent practicable."

The Senate Armed Services Committee approved a similar provision in June of this year. Although the Senate has yet to consider the House-passed version of the NDAA, it appears likely to do so and the final law is likely to include a provision requiring the President to study ways to control the spread of "cyber weapons." A statement published by the House Armed Services Committee about the 2014 NDAA emphasized the need for a review of export controls on "cyber weapons" and noted the importance of including industry in such a review:

> The Senate committee-reported bill contained a provision (sec. 946) that would require the President to establish an interagency process to develop policy to control the proliferation of cyber weapons through unilateral and cooperative export controls, law enforcement activities, financial means, diplomatic engagement, and other means that the President considers appropriate. The provision would also require the President to develop a statement of principles regarding U.S. positions on controlling the proliferation of cyber weapons to create new opportunities for bilateral and multilateral cooperation to address this shared threat. The provision would require the interagency process to produce recommendations within 270 days of the enactment of this Act. The House bill contained no similar provision. The agreement includes the Senate provision with an amendment that would require the President, to the extent practicable, to provide for industry participation in the interagency process.[3]

Efforts to place export controls on devices and software used for penetration testing, for example, could create substantial compliance challenges for US cybersecurity businesses that outsource some of their software and hardware development or that do not currently need export licenses for sales abroad.

It is important that any new regulatory requirements be workable, so companies that may be affected by increased export controls in this area will want to monitor developments closely and comment on proposed export control changes that could impose new hurdles for the global cybersecurity industry.

---

[1] A copy of the public statement from 2013 "Wassenaar Arrangement" meetings can be found here.

[2] A copy of the bill text can be found here.

[3] A copy of the House Armed Services Statement can be found here.

Authors

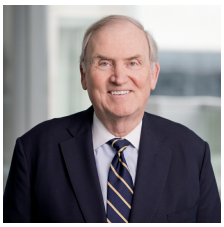
Jamie Gorelick

PARTNER

Chair, Regulatory and Government Affairs Department

jamie.gorelick@wilmerhale.com

+1 202 663 6500



Ambassador Robert M. Kimmitt

SENIOR INTERNATIONAL COUNSEL

Co-Chair, Crisis Management and Strategic Response Group

robert.kimmitt@wilmerhale.com

+1 202 663 6250

Ronald I. Meltzer

SENIOR COUNSEL

ronald.meltzer@wilmerhale.com

+1 202 663 6389

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195