Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

July 20, 2015

Via email to publiccomments@bis.doc.gov

Kevin J. Wolf
Assistant Secretary for Export Administration
Regulatory Policy Division, Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC 20230

Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (Docket No. 150304218-5218-01; RIN 0694-AG49)

Dear Assistant Secretary Wolf:

I am writing today on behalf of Cisco Systems (Cisco) in response to the request for comment on a Proposed Rule from the Department of Commerce's Bureau of Industry and Security (BIS) dated May 20, 2015. The Proposed Rule seeks "to implement the agreements by the Wassenaar Arrangement (WA) at the Plenary meeting in December 2013 . . . ." It would have the effect of regulating a wide array of technologies used in security research as controlled exports, in the same manner as if they were munitions.[1] We have identified a number of significant concerns that we believe require BIS to revisit the text of the Proposed Rule.[2]

---

[1]Specifically, the rule would cover: "systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software; technology required for the development of intrusion software; 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."

https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

[2] The two issues discussed below (export controls on unpublished vulnerabilities and the demand for source code) are intended to illustrate the nature and depth of our concerns. Cisco has additional concerns and may seek to supplement the record based on whether and how BIS moves forward with the Proposed Rule.

Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

BIS' focus on limiting the cross-border trafficking of weaponized software is well-intentioned, but the current text would cause significant unintended consequences that must be addressed in a revised draft of the Proposed Rule. If implemented in its current form, the Proposed Rule would present significant challenges for security firms that leverage cross border teams, vulnerability research, information sharing, and penetration testing tools to secure global networks, including Cisco. The result would be to negatively impact—rather than to improve—the state of cybersecurity.

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. In order to develop, deliver, manage, and maintain the innovative products and services that Cisco's customers count on to run their businesses, we must engage in complex security research. This requires Cisco to develop and deploy security systems that include intrusion detection, intrusion prevention, next generation firewall, endpoint monitoring, dynamic file capture and analysis, application identification and control, identity management and analysis, and deep content inspection and analysis systems that operate across the extended network and devices.

We need the ability to attack, assess, and strengthen our own technology using sophisticated penetration testing tools. We also rely upon information about unpublished vulnerabilities that we find or that are brought to our attention by outside researchers. In the course of these efforts, we welcome and readily coordinate with expertise from around the globe—and work around the clock.

This level of commitment is necessitated by a dynamic threat environment populated by dedicated, well-resourced adversaries seeking to compromise and undermine the effectiveness of our security investments. These same adversaries can and do readily engage in subversive behaviors. If they discover vulnerabilities before Cisco does, attackers will seek to compromise networks with the intent of controlling systems and manipulating people for their own gain. Many of the activities required to respond to these threats would be restricted or subject to onerous export licensing requirements if the Proposed Rule were adopted.

We understand the importance of the government's concerns regarding the unregulated export of weaponized software. However, many of the same techniques used by attackers are important to developers testing their defenses and developing new effective responses. Cisco needs access to the very tools and techniques that attackers use if we have any hope of maintaining the security of our products and services throughout their anticipated lifecycles. The development of new export control requirements must, therefore, be done carefully and based upon the needs of legitimate security researchers. Otherwise, we will

Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

leave network operators blind to the attacks that may be circulating in the criminal underground—and ultimately blind to the very weaponized software that the proposed rule intends to constrain.

It is our hope that based upon the comments received to the Proposed Rule, BIS will reconsider the text and offer a revised draft. As it does so, there must be a recognition that the success of the IT industry depends upon a global development model. It is unrealistic to expect that all of the resources necessary to secure complex networks will sit inside one country. Implementation of the current text would unnecessarily restrict the sharing of research between teams that work globally in response to discovered threats and vulnerabilities.

Cisco believes the Proposed Rule could stunt the development of valuable avenues of security research—even as attackers continue to innovate freely. BIS has responded to such concerns by pointing out that researchers seeking to export information about unpublished vulnerabilities could take advantage of an exception in the Export Administration Rules (EAR) for information that is already public. According to an FAQ published by BIS: "[u]nder Section 734.7 of the EAR, information that is published, or released at an open conference, is not subject to the EAR."

The publication of previously unpublished vulnerabilities is not a substitute for reasonable export license exceptions—and could actually cause significant harm to Cisco's security efforts. Absent adequate license exceptions enabling the security community to quickly share and respond to vulnerability information, the current text would create perverse incentives to publish information about vulnerabilities before developers can mitigate or patch the affected technology. The Proposed Rule could, therefore, unintentionally incentivize the routine publication of previously unknown vulnerabilities without coordination, which would ultimately lead to more zero day exploits.

The security community shares vulnerability information to develop and disclose fixes in a coordinated way. The Department of Commerce's own National Telecommunications and Infrastructure Administration (NTIA) recently stated that such coordination is so important that it is launching a multistakeholder process entitled "Enhancing the Digital Economy Through Collaboration on Vulnerability Research Disclosure" this September.[3] BIS needs to rework its proposal to support NTIA's efforts. At a minimum, any future iteration of the Proposed Rule should include clear definitions of the controlled items and provide explicit

[3] http://www.ntia.doc.gov/blog/2015/enhancing-digital-economy-through-collaboration-vulnerability-research-disclosure

Cisco Systems, Inc.
601 Pennsylvania Ave, NW

Direct: 202 354-2904
FAX: 202 354-2930
www.cisco.com

license exceptions enabling legitimate security researchers to share and respond to vulnerability information in a timely manner.

We are also concerned that the proposal calls for the disclosure of source code to the U.S. government. Supplement No. 2 to Part 748—Unique Application and Submission Requirements would require applicants: "[u]pon request, [to] include a copy of the sections of source code and other software (e.g., libraries and header files) that implement or invoke the controlled cybersecurity functionality." As the U.S. Government is well aware, developers of information technologies are increasingly facing demands by other governments for disclosure of our intellectual property. Any proposal from the U.S. Government regarding source code disclosure production requirements is extremely damaging.

The concerns listed above are examples demonstrating that the scope of the requirements in the Proposed Rule are far broader than necessary to address BIS' stated intent—controlling the export of weaponized software. We look forward to working with the Department of Commerce to ensure that the goals of the proposal can be met in a manner that is technology neutral, narrowly tailored to the actual risks faced by the nation, and reflective of the needs of legitimate security researchers seeking to protect the information technologies upon which we increasingly rely. We look forward to continuing the conversation.

Best wishes,

Eric Wenger

Eric Wenger, Director Global Government Affairs
Cybersecurity and Privacy Policy
Cisco Systems