

July 20, 2015

Ms. Catherine Wheeler
Director, Information Technology Control Division
Bureau of Industry and Security
U.S. Department of Commerce
1401 Constitution Avenue NW
Washington, DC 20230

Dear Ms. Wheeler:

The Information Technology Industry Council (ITI) welcomes the opportunity to provide its views on the proposal by the Bureau of Industry and Security (BIS) to implement stricter export controls on certain “cybersecurity” products – namely those interacting with “intrusion software” – identified in 2013 by the Wassenaar Arrangement. While we support the human rights objectives inspiring this effort under Wassenaar, we have significant concerns regarding the commercial and security implications of this proposed means of achieving them. We look forward to working with you and your colleagues to address these concerns.

ITI is the global voice of the information and communications technology (ICT) industry. Our members include the world’s leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI advocates policies that advance industry leadership in technology and innovation, open access to new and emerging markets, promote e-commerce expansion, protect consumer choice, and enhance the global competitiveness of its member companies.

A central element of our advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not just to the ICT sector but to the global economy as a whole. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to conduct research and development, design and manufacture goods, and market and distribute products and services to their customers. U.S. and global ICT companies also have a long history of exchanging security-related information across borders with users, customers, governments, and other stakeholders, which helps them protect their own systems and maintain high levels of security for the technology ecosystem as a whole.

The Obama Administration has consistently recognized the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. Earlier this year, President Obama issued [Executive Order 13691](#), which, among

other things, states that “private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.” We are concerned that the proposed rule could undermine this key Administration principle and severely complicate the ability of companies in all sectors to protect and enhance their security.

As an initial matter, the proposed rule presumes clear lines of demarcation between “intrusion software” (not controlled) and “software that generates, delivers, or communicates with intrusion software” (controlled). However, subject matter experts do not agree on whether this line exists in reality or, if it does, exactly where it lies. The natural consequence for compliance-driven exporters would be to assume a very conservative position by “playing it safe” and assuming that large volumes of software/technology would be controlled. The natural consequence for BIS would be unpredictable (but likely large) volumes of license applications.

Similarly, the overall breadth of the draft measure would mean that companies could be required to apply for and obtain literally thousands of export licenses to cover the vast range of information-sharing and other security-related activities that they undertake involving the movement of data across borders (in areas such as product development, security testing and research) and the proper securing of their own and their clients’ information and networks. It would be extremely burdensome and costly for individual companies to prepare license applications and for BIS to review and rule on them. It would also be extraordinarily time-consuming. Months could pass between the time that the need to share threat information arises and the time permission to do so is granted. Meanwhile, potential vulnerabilities could be exploited many times over.

The proposed measure would be harmful even at the level of individual companies as it relates to their own internal data sharing and cybersecurity operations. A single company might need to obtain large numbers of licenses for its headquarters to share certain security information, software and tools with overseas affiliates or use certain products to insure the security of its internal network. Even domestically, a manager at headquarters might need to obtain a license to walk down the hall and discuss certain security issues or development of new tools with a team member who is a national of a country other than the United States or Canada.

In addition, there are potentially broader international ramifications of pursuing such policy approaches. Whatever the rationale, the broad scope of the proposed rule would be seen as the imposition of government restrictions on cross-border data flows. Such rules would provide a precedent for other governments to expand their own limitations on the flow of information across borders, including on the basis of “security,” to the detriment of global trade and U.S. companies operating in those markets.

In sum, BIS’ proposed rule would not only impose tremendous costs on some of the United States’

leading innovators and job-creators. It would also directly undermine efforts to achieve the Administration's objectives for enhancing commercial information security, both of the companies covered by the regime and the global ICT ecosystem generally.

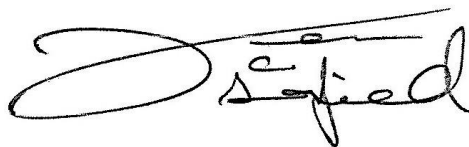
We urge BIS to cease consideration of this harmful proposed measure and immediately engage the U.S. ICT industry and other stakeholders in detailed consultations regarding how best to achieve the human rights objectives of the Wassenaar Arrangement without compromising the security objectives of both the Administration and the ICT industry. Such consultations would allow government and industry to discuss preferable steps to take, including, but not limited to:

- establishing a working group of technical experts from government and industry to systematically address the technology and cybersecurity considerations at issue;
- providing for a self-executing license exception mechanism under section 740 of the Export Administration Regulations (EAR) that does not include reporting requirements and is structured to enable exporters to export, re-export, and transfer (including in-country transactions) systems, equipment, components, technology, and/or software for internal company use worldwide;
- maintaining relevant provisions of the encryption (ENC) exception, to avoid placing unnecessary burdens on companies' security operations and innovation capabilities; and
- providing for an "intra-company license exception" that would allow for information sharing, internal company use of security products, and end user controls that do not block legitimate permissible uses.

We would be pleased to discuss other ideas for achieving our shared objectives in this regard.

Thank you for your consideration of these comments. We look forward to working with you and your colleagues further on these important issues.

Sincerely,



Dean C. Garfield
President and CEO

cc: Kevin Wolf, Assistant Secretary for Export Administration
Matthew Borman, Deputy Assistant Secretary for Export Administration
Hillary Hess, Director Regulatory Policy Division, Office of Export Services