Written Testimony of

Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the

Subcommittee on Information Technology
Committee on Oversight and Government Reform

And

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

U.S. House of Representatives

Wassenaar: Cybersecurity and Export Control

January 12, 2016

Written Testimony of
Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the
Subcommittee on Information Technology
Committee on Oversight and Government Reform

And

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives

Wassenaar: Cybersecurity and Export Control

January 12, 2016

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond, and members of the subcommittees, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before your subcommittees today on the important topic of the Wassenaar Arrangement and the implications for cybersecurity of imposing stricter export controls pursuant to the Bureau of Industry and Security's (BIS') proposed rule, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, released in the *Federal Register* on May 20, 2015 (the "Proposed Rule").[1] While we strongly support the Wassenaar Arrangement's human rights objectives of addressing the export and proliferation of weaponized malicious software, we have significant concerns regarding the commercial and security implications of this proposed means of achieving them. We welcome your interest and engagement on this subject.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity is critical to our members' success—the protection of our customers, our brands, and our intellectual property is an essential component of our business, and affects our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business in countries

[1] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries across the globe, servicing customers that typically span the full range of global industry sectors, such as banking and energy. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

I will focus my testimony on four areas: (1) The critical importance of cross-border data flows to cybersecurity; (2) the potential impacts of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on our companies' cybersecurity and innovation efforts; (3) the broader effects of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on ecosystem cybersecurity for all industries; and (4) recommendations on how to best achieve the objectives of the Wassenaar Arrangement without compromising security objectives.

Cross-Border Data Flows and Cybersecurity

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also 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 enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing 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 geographically-dispersed employees, 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.

Indeed, as well as facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for companies globally, helping to secure the systems and networks that manage production schedules and Human Resource (HR) data, as well as communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe. The Proposed Rule is part of a troubling global trend of erecting barriers to the free movement of global data, as also exemplified in the recent European court of Justice opinion effectively invalidating the Safe Harbor agreement.

Perhaps even more disturbing, the Proposed Rule, and the trend of impeding data flows generally, is contrary to the thrust of current U.S., and indeed global, cybersecurity policy.

To illustrate, as you know, late last year, Congress passed a bipartisan cybersecurity threat information sharing bill, the Cybersecurity Act of 2015.[2] The bill acknowledges that voluntary sharing of information

[2] Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N (2015).

regarding cyber threats, with appropriate privacy safeguards, is an integral component of improving our cybersecurity ecosystem, as it helps all stakeholders better protect and defend cyberspace. More specifically, Section 103 requires the heads of various federal security agencies to jointly develop procedures to ensure the Federal Government maintains "a real-time sharing capability." Section 105 directs the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government receives and shares information about cyber threats, including via an automated real-time process, and Section 203 requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. President Obama signed the law, which aligns with the Administration's consistent recognition of the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. For instance, also last year, President Obama issued Executive Order 13691,[3] which, among other things, states, "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."

All of these policy efforts are intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity, and all of these initiatives contemplate the sharing of cybersecurity threat information as inclusive of information related to vulnerabilities. Given that the overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity, we are concerned that the Proposed Rule and the 2013 additions to the Wassenaar Arrangement could undermine this key principle and severely complicate the ability of companies in all sectors and government entities to share information in real-time to protect and enhance their security.

The onerous licensing scheme contemplated by the Proposed Rule, however, would necessarily slow down the sharing of vulnerability information (both intra-company and between companies). In other words, because the Proposed Rule is effectively erecting additional barriers to vulnerability sharing, it appears diametrically opposed to the goals of multiple cybersecurity policy initiatives recently advanced by U.S. government policymakers.

Potential Impacts of the Proposed Rule on Tech Sector Innovation and Cybersecurity Efforts

The Proposed Rule would significantly damage cybersecurity technology innovation efforts by burdening companies with the onerous and time consuming process of applying for large volumes of unnecessary licenses. The damage could potentially impact a wide range of cybersecurity products and technologies in development, such as innovative defensive cybersecurity products, in addition to potentially restricting research into cyber vulnerabilities and exploits connected to valuable internal business activities, such as research and testing to determine vulnerabilities in our companies' systems, products and technologies. Both of these sets of activities are intended to strengthen the cyber defenses of our companies and customers worldwide. At a minimum, the licensing scheme envisioned by the Proposed Rule would negatively impact the ability of companies in the U.S. seeking to develop such tools, and

[3] Exec. Order No. 13,691, 80 Fed. Reg. 9347 (February 20, 2015), *available at* https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.

would almost certainly leave critical data systems much less protected, and subject to increased cyberattacks or breaches by malicious actors, because of the inevitability of delays associated with applying for and receiving approvals for license applications.

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 actually exists, and 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 or 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 both individual companies to prepare license applications as well as for BIS to review and rule on them. It would also be extraordinarily time consuming. Months could pass between the time 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 Rule would be harmful to 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.

While concerning for any company doing business globally, the problems would disproportionately impact many companies in the tech sector, particularly companies developing software deployed across industry networks and the cloud, and security companies working to innovate solutions to help protect all stakeholders' networks and systems.

Also troubling for these companies is language in the Proposed Rule empowering BIS to make the granting of licenses contingent upon companies' disclosing their source code. The Proposed Rule states, "when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled cybersecurity functionality." We strongly urge BIS to reconsider any requirement that applicants hand over their source code. This is particularly important at a time when U.S. officials and industry are urging foreign governments not to compel vendors to turn over intellectual property, such as source code and other sensitive corporate data.

Broader Impacts of the Proposed Rule on Cybersecurity across Industry

Concerns regarding the Proposed Rule do not only impact the technology sector – they will negatively impact the ability of all companies to defend themselves from cybersecurity threats. All sectors, especially critical infrastructure, need effective cybersecurity, including the ability to share information quickly within sectors, among other sectors and with the Federal government, to discover and close vulnerabilities before they are widely known.

To be able to detect and remediate vulnerabilities – whether in products or systems – companies must retain the ability to identify and test those vulnerabilities. Even products that are not "specially designed" to perform the single intrusion function may be captured under the breadth of the Proposed Rule.

Most fundamentally, the Proposed Rule would do more to damage, rather than improve, the cybersecurity of U.S. companies, by restricting access to protective security measures required by networks all around the world. Imposing significant constraints on the ability of multinational corporations across multiple sectors to take cyber self-defense actions seems to belie common sense. For instance, companies' vulnerability assessment teams use "intrusion software" to identify and track vulnerabilities in network devices and applications. The ability of companies to perform this activity across global boundaries, by sharing vulnerability information amongst their own-geographically dispersed or multi-national employees, should not be impeded.

Collaboration is most urgently needed during ongoing attacks. As stated above, the entire point of passing information sharing legislation was to facilitate the sharing of cybersecurity threat information, including information regarding security vulnerabilities, in as close to "real time" as possible so as to more quickly remediate them and minimize potential damage to companies' networks. Potentially high-risk vulnerabilities are most valuable to hackers, and so are the exact type of cyber weaknesses that companies want to find during their internal penetration testing. Injecting a licensing scheme, with onerous requirements precluding intra-company transfers of critical cybersecurity threat information that would prevent companies from taking necessary defensive actions across their worldwide networks, seems to make little sense.

This problem is exacerbated by the Proposed Rule's "policy of presumptive denial" for zero-day and rootkit capabilities, e.g., "product or system" or "delivery tool."[4] Presumptive denial would greatly restrict businesses' abilities to share threat information and counter some of the most dangerous cyber vulnerabilities and exploits. Detailed technical data on the origins of a previously unknown vulnerabilities, or zero-days, is the very same information that enables bad actors to exploit weaknesses in companies' computer systems. If there is no technical difference defined in the Proposed Rule between the cybersecurity activities performed by our companies and the criminal activities performed by hackers, our companies will be significantly hampered by the imposed controls.

[4] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28855 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

For the same reasons, the proposed export control regime could also impose severe limitations on information sharing beyond the walls of companies themselves, impacting established cybersecurity information sharing best practices more generally, including sharing within public-private partnerships (e.g., sector-coordinating councils and information-sharing and analysis organizations), and sharing linked to government contracts and protected programs. For example, information that is shared with the U.S. government voluntarily (e.g., US-CERT) or as required under contracts (e.g., FISMA and FedRAMP) could be thrown into question, which would benefit neither the government nor the private contractor.

Additionally, the portions of the Proposed Rule restricting surveillance items might also impact established best cybersecurity practices of companies. For instance, many companies utilize some type of packet analyzer (i.e. packet sniffer) to monitor and capture digital traffic passing over a network so that technicians can identify malicious code. The 2013 amendments to the Wassenaar Arrangement added the following to the list of dual-use goods: "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."[5]

It is unclear how the inclusion of the restriction regarding IP network communications might impact the ability of companies to deploy their monitoring equipment and software in multiple locations on their networks to fight bad actors. Imposing licensing requirements that could impact such smart and basic cybersecurity practices seems both unfeasible and detrimental to enterprise security.

Recommendations

The Proposed Rule raises a host of complex and interrelated technical policy issues involving usually disparate topics including cybersecurity, export control law, and human rights, and impacts government and industry interests alike. Given the diversity of impacted and knowledgeable stakeholders in these divergent areas, public-private collaboration in this issue area would greatly enhance the expertise of federal government representatives both at Wassenaar and in any future rulemakings.

Thus, at a minimum, we urge BIS to withhold publication of the Proposed Rule, and forgo further revisions with an eye toward implementation, and to instead engage the U.S. ICT industry, its inter-agency partners, and other stakeholders in detailed consultations regarding how best to achieve the 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 options and what further steps to take (likely in parallel) including, but not limited to:

- **Returning to Wassenaar to reopen the control, and in the interim, withholding the rule from publication.** Renegotiating the agreement is certainly a better option than simply not implementing the rule, which seems neither a prudent nor practical option. However, given that there appears to be wide variation amongst Wassenaar signatories in the implementation

[5] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

of the particular provisions impacting cybersecurity, clarifying the Wassenaar Agreement language itself seems the surest means of ensuring consistent implementation in a global cybersecurity environment.

- **Establishing a working group of technical experts from government and industry to systematically address both the technical and policy aspects of the cybersecurity, human rights and export controls considerations at issue**. As stated above, the Proposed Rule implicates competing equities and impacts multiple stakeholders. With this is mind, we call for the formation of an experts group to represent these competing interests and fully analyze the multiple facets of implementation of the 2013 Wassenaar Arrangement Plenary Agreement. We believe the experts group should have a broad charter and could examine any number of topics, including:
    - *Options for targeted implementation.* If reopening the control at Wassenaar proves unsuccessful and the U.S. has no choice but to implement the Proposed Rule, it is essential to work with security experts from government agencies and industry to devise an appropriate, targeted solution in consideration of all the dimensions of this important issue, so as to minimize the broader impacts. In particular, we advise examining how to limit the scope and coverage of the Proposed Rule via a narrower definition to avoid disrupting day-to-day business and security operations of global companies.
    - *Applicability of Pre-Existing Rules.* The experts group might explore whether any pre-existing rules might be applicable, or able to be modified, to address some of the legitimate human rights concerns underlying the rule.
    - *Targeting Bad Actors.* Exploring whether there is a way to target bad actors, as opposed to the current approach, which targets the technology. The experts group could focus on the variance between "defensive" and "offensive" cybersecurity measures, in an effort to differentiate between "white hat" developers who are seeking to improve security across the ecosystem and "black hat" hackers who are focused on substantially harming an information system or data on an information system. Enabling BIS to set appropriate export controls based on malicious end use which do not inadvertently subject companies, researchers and others to burdensome and onerous internal licensing requirements in order to conduct day-to-day business would be a win.

Conclusion

Members of the subcommittees, ITI and our member companies are pleased you are examining how the Wassenaar Arrangement will affect the cybersecurity of our nation and private industry. The ICT sector is innovative and dynamic, continuously evolving as new products are developed and existing technologies are improved. However, the threats to our security also constantly change. Criminals and other bad actors modify and adapt their techniques almost as quickly as the industry is constantly innovating to address those threats. However, for our security efforts, and those of the federal government, to be effective, any cybersecurity regime implemented by government bodies must be flexible to allow government and private industry systems to leverage new technologies and business models, address constantly changing threat dynamics and manage new risks and vulnerabilities.

In addition, there are potentially broader international ramifications of pursuing policy approaches such as those embodied by the Proposed Rule. Whatever the rationale, the broad scope of the Proposed Rule could be viewed 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. Doing so would not only impose tremendous costs on some of the United States' leading innovators and job-creators, but 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 stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to achieve the objectives underlying the Wassenaar Arrangement while also collectively improving cybersecurity innovation, risk management, and resilience.

Thank you.