Before the
DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Washington, DC 20230

In the Matter of	)	
	)	
Amendment of Parts 740, 742, 748, 772,	)	Docket No. 150304218-5218-01
and 774 of the Wassenaar Arrangement's	)	
2013 Plenary Agreements Implementation	)	
regarding Intrusion and Surveillance Items	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7714

July 20, 2015

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
Bureau of Industry and Security
Washington, DC 20230

In the Matter of	)	
	)	
Amendment of Parts 740, 742, 748, 772,	)	Docket No. 150304218-5218-01
and 774 of the Wassenaar Arrangement's	)	
2013 Plenary Agreements Implementation	)	
regarding Intrusion and Surveillance Items	)	

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

I. Introduction and Summary

The Telecommunications Industry Association ("TIA") hereby submits comments in response to the Department of Commerce Bureau of Industry and Security's ("BIS") request for comment to inform BIS' implementation of the Wassenaar Arrangement ("WA") export control December 2013 Plenary agreements over "cybersecurity items."[1]

TIA represents hundreds of ICT manufacturer, vendor, and supplier companies in government affairs and standards development. Numerous TIA members are companies producing ICT products and systems, creating information security-related technologies, and providing ICT services information systems, or components of information systems. These products and services innovatively serve many of the critical infrastructure sectors directly impacted by the BIS proposal. Representing our membership's commitments in this area, TIA also holds membership and is actively engaged in key public-private efforts that contribute to secure information systems,

[1] *See Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items,* 80 Fed. Reg. 28853 (May 20, 2015) ("BIS Proposed Rule").

including the CSRIC; the Communications Sector[2] and Information Technology Sector[3] Coordinating Councils; and the National Coordinating Center for Communications ("NCC"), the Information Sharing and Analysis Center ("ISAC") for telecommunications, part of the Department of Homeland Security's ("DHS") National Cybersecurity and Communications Integration Center.[4]

Through its Cybersecurity Working Group, TIA members engage in policy advocacy consistent with the following principles:

- Public-private partnerships should be utilized as effective vehicles for collaborating on current and emerging threats.
- Industry-driven best practices and global standards should be relied upon for the security of critical infrastructure.
- Voluntary private sector security standards should be used as non-mandated means to secure the ICT supply chain.
- Governments should provide more timely and detailed cyber intelligence to industry to help identify threats to protect private networks.
- Cybersecurity funding for federal research efforts should be prioritized.

TIA appreciates BIS' efforts to create a transparent and inclusive multistakeholder process to address key cybersecurity challenges and looks forward to working with the BIS and other governmental stakeholders, both directly and through the envisioned multistakeholder process moving forward. In comments below, TIA:

- Urges BIS to provide needed definitional clarifications;
- Urges BIS to avoid unnecessary restrictions on the sharing of information within and among organizations;

---

2 http://www.commscc.org/

3 http://www.it-scc.org/

4 http://www.dhs.gov/national-coordinating-center-communications

- Provides input on the proposed ability of BIS to require source code from newly-covered items under this WA expansion; and

- Provides answers to select questions posed by BIS related to the impact of the proposal.

II. GENERAL VIEWS ON ISSUES RAISED BY BIS PROPOSAL

Initially, TIA notes that it shares the WA's goal of improving regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulation and use by bad actors. Further, TIA appreciates the importance of the concerns underlying the WA regarding the production, export, and utilization of weaponized software. However, many of the techniques used by attackers through this software are important to defenders seeking to test their defenses against intrusion. Therefore, TIA strongly urges BIS to move forward only after careful consideration of and deliberation on the views of impacted shareholders before implementing the WA.

TIA has long urged the United States government that it should not enact policies within the United States which would unduly restrict trade in ICT equipment and software. Across numerous contexts, other countries have cited similar concerns regarding foreign ICT equipment and are currently considering overly-broad and/or overly-restrictive trade measures. If these countries adopt such policies, the United States' global economic competitiveness could be severely adversely affected. TIA urges BIS to recognize that the success of the United States' ICT industry depends upon a global development model.

The global ICT industry relies upon a flexible supply chain that is characterized by intense competition, price fluctuation, and supply of different inputs. Since hardware and software products and components may be designed, aggregated, tested, and finalized in different locations, it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. Therefore, the focus of any product security concerns must always be on whether the product is secure, not on the country of origin. It is frankly unrealistic to expect that all of the resources necessary to secure complex networks will reside inside of one country.

Further, in the interest of protecting innovation from technologically discriminatory policies and regulations, TIA strongly urges BIS to remain true to the principle of technological neutrality. While it is important for the United States to honor its commitments and help ensure greater international security, it must not do so at the expense of the critical technological advantages created and enjoyed by the innovative freedom and spirit of the ICT industry.

A. BIS Should Clarify Key Definitional/Scope Terms

TIA believes that definitional clarity is crucial to the successful discussion or implementation of any regulatory regime. Any uncertainty could lead to hesitation and, potentially, greater market disruption. These disruptions can manifest as increased use of resources on legal compliance, licensing fees, etc., rather than research and development. For example:

- While BIS has noted that Category 4 control entries would govern "the command and delivery platforms for generating, operating, delivering, and communicating with 'intrusion software'" as well as "the technology for developing 'intrusion software,'" the rules would not cover "intrusion software" itself.[5] As a result, "transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware" would not fall under the BIS controls.[6] In reviewing the proposed BIS rule, TIA fears that, in practice, making a distinction between the "platform" for the intrusion software and the intrusion software itself will be intensely difficult. For example, because companies that develop software for products and services require the use of basic tools such as operating systems (and hardware compatible with those operating systems), these basic tools could be interpreted as falling under the BIS rule. We do not believe such a wide scope to be in the interest of the WA and urge for BIS to engage with stakeholders towards providing further written clarity on this aspect of the proposal before any new export requirements are finalized.
- TIA urges for BIS to more clearly define the meaning and scope of "communication with" intrusion software means.[7] Based on the BIS proposal, TIA believes this key term to be over-inclusive, and impacted organizations are likely to have difficulty determining the limits of this term.

---

5 FAQ

6 *Id.*

7 BIS Proposed Rule at 28554.

- As another example, the BIS proposal would extend over "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."[8] TIA members use IP network communications surveillance to track, anticipate, and counteract intrusion software attempting to breach their systems. As proposed, BIS would be inserting itself into, and impeding, this essential and widely-used network security practice. TIA believes that this aspect of the BIS proposal should be as narrowly scoped as possible to address BIS' interests without harming basic network security management for the private sector through revisions to make clear that the rule will not impact companies' ability to monitor their own networks to detect and mitigate nefarious intrusions.

B. TIA Urges BIS to Avoid Unnecessary Restrictions on the Sharing of Information within and among Organizations

BIS proposes that all exports of specified systems, equipment, components or software that would generate, operate, deliver or communicate with 'intrusion software' would require an export license under the proposed rule.[9] Notably, BIS has also stated that, as proposed, the new WA rules contain "no license exception for intra-company transfers or internal use by a company headquartered in the United States under the proposed rule."[10]

As noted above, in an era of globalized ICT development and sales, countless TIA members conduct tests on both hardware and software at locations around the globe. TIA believes that, as proposed, this aspect of the BIS proposal would place licensing requirements (or, at minimum, a need for the seeking of exemptions) on a nearly endless amount of company internal transactions that are necessary in the development of hardware and software products and services. If ICT companies in the United States were forced to gain approval for every single test performed outside of the United States, as is implied by this definition, the security of American business would, inevitably, be severely undermined. The impact of this policy would place significant resource and time delays into the product development cycle where intra-

---

8 *Id.*

9 BIS Proposed Rule at 28854. Term used is "Systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computers and network-capable devices"

10 http://www.bis.doc.gov/index.php/policy-guidance/faqs

organization software development teams share information, collaborate on code development, and distribute work product. In short, TIA believes that the lack of an exception in the BIS for intra-company transfers or internal use will present an untenable environment for companies that develop network security products and services, and we urge BIS to further engage with stakeholders towards a revised, and more feasible, application of the WA.

Furthermore, TIA notes that BIS proposal in this context may conflict with established Federal policy regarding the sharing of cybersecurity threat information among key stakeholders, both public and private. The United States government, in partnership with industry members from across critical infrastructure sectors, remains committed to the sharing of timely cybersecurity threat information through the NCCIC/Comm-ISAC (see above). In the last few years alone, the Administration has undertaken a number of important activities to improve cyber defenses, enhance response capabilities, and upgrade incident management tools in both the private and public sectors.[11] As just one recent example, Executive Order 13691 took steps to improve the sharing of timely cyber-based threat information amongst and between government and industry stakeholders through the establishment of Information Sharing and Analysis Organizations ("ISAOs").[12] TIA, along with countless other public and private stakeholders, strongly believes that as the number and diversity of cyber threats to both the public and private sectors continue to increase, it is more important than ever for the enablement of voluntary real-time bi-directional sharing in any way possible. The impact of this BIS proposal clearly complicates, thereby impeding, this information sharing by forcing licensing requirements and associated liability concerns into the process. BIS is encouraged to closely coordinate with other Federal stakeholders as well as industry to ensure that the collaborative environment being striven for is not disrupted.

C. Proposal to Require Sharing of Source Code for Licensed Items

As written, BIS would, upon request, be able to demand that the licensing applicant include "a copy of the sections of source code and other software (e.g., libraries and header

---

[11] *See*, *e.g.*, https://www.whitehouse.gov/the-press-office/2015/07/09/fact-sheet-administration-cybersecurity-efforts-2015

[12] *See* Exec Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing (February 13, 2015), available at https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing ("EO 13691").

fields) that implement or invoke the controlled cybersecurity functionality."[13] Across contexts, TIA strongly opposes proposals that would require the escrowing of source code in order to gain access to markets. Product source code represents the highest level of business confidentiality for the ICT industry, and requiring the disclosure of these codes is a strong incentive not to invest in crucial research and development. Further, such a policy may have the impact of forcing the movement of development teams to locations outside of U.S. jurisdiction to avoid this policy. While TIA understands that requiring source code of some encrypted items is an existing requirement under BIS rules implementing the WA, we strongly urge BIS not to extend this requirement to items contemplated under this rulemaking.

Sovereign interest in a secure and development-friendly cyber economy is best served, in any country, by policies that encourage competition and customer choice. In numerous contexts internationally, TIA members continue to face anticompetitive proposals that include mandatory escrowing of source code. We strongly urge BIS to ensure its proposals are consistent with established USG policy, and to contemplate the impact such a policy would have on other governments that look to the United States as an example of prudent regulatory behavior. Further, TIA requests that BIS clearly justify why it would need to review such business confidential information to accomplish their goals under the WA.

[13] BIS Proposed Rule at 28855.

III. TIA RESPONSES TO SELECT QUESTIONS POSED IN THE BIS REQUEST FOR COMMENT

a. *How many additional license applications would your company be required to submit per year under the requirements of this proposed rule? If any, of those applications:*

1. *How many additional applications would be for products that are currently eligible for license exceptions?*
2. *How many additional applications would be for products that currently are classified EAR99?*

Due to the sweeping expansion proposed by BIS, many companies should expect to see a significant increase in the number of licenses based on the requirements under the proposal as written. As described above, the impact of this proposal would interfere in all phases of product development, from the initial stages of research and development to the shipment of final products. For larger companies, the increase in needed licenses could be in the thousands.

***

b. *Would the rule have negative effects on your legitimate vulnerability research, audits, testing or screening and your company's ability to protect your own or your client's networks? If so, explain how.*

Based on the wide reach of the definition of "intrusion software," the BIS rule as proposed would have profoundly negative effects on legitimate vulnerability research, audits, testing, and screening of company networks as well as those of their clients. As noted above, due to the global nature of the ICT industry, many tasks required by vulnerability assessment teams would potentially require licenses on a per-communication basis, not only for those developing "intrusion software," but also for those developing or using a system that "communicates with" intrusion software.

In addition to governing transactions across geographic borders, the proposed BIS rule would implicate transactions within a single room should one of the employees be of a nationality other than the U.S. or Canada. The interruptions and costs associated with implementing BIS' proposal would not only reduce the ability of companies to invest and

innovate, but would also result in delayed mitigation of network vulnerabilities that are identified. It is crucial that BIS refrain from interfering in the intra-organizational development of network intrusion tools and products. In addition to the impact of the companies seeking the license themselves, the BIS proposal would also have a similar trickle-down effect on trusted third-party contractors, whether in the product development cycle or in a post-deployment security audit.

We note that the BIS proposal runs counter to the existing public-private partnerships used across critical infrastructure sectors to share timely cybersecurity threat information. Finally, TIA wishes to underscore the negative example the proposed approach would set in the international community where the private sector continually contends with country-specific discriminatory economic policies.

IV. CONCLUSION

Based on the concerns listed above, we believe that the stated intent of the proposed regulations appears significantly different than the scope of the actual requirements. 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 are narrowly tailored to the actual risks faced by our nation.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Brian Scarpelli
Director, Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 North Courthouse Rd.
Suite 200
Arlington, VA 22201
(703) 907-7700

July 20, 2015