July 20, 2015

Ms. Hillary Hess
Director, Regulatory Policy Division
Room 2099B
Bureau of Industry and Security
U.S. Department of Commerce
14th Street & Pennsylvania Ave., N.W.
Washington, D.C. 20230

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (*Federal Register* Notice of May 20, 2015; RIN 0694-AG49)

Dear Ms. Hess:

The Semiconductor Industry Association ("SIA") is the premier trade association representing the U.S. semiconductor industry. Founded in 1977 by five microelectronics pioneers, SIA unites over 60 companies that account for nearly 90 percent of American semiconductor production. The semiconductor industry accounts for a sizeable portion of U.S. exports.

SIA is pleased to submit the following public comments in response to the request for public comments issued by the Commerce Department's Bureau of Industry and Security ("BIS") on proposed revisions to the Export Administration Regulations ("EAR") pertaining to intrusion and surveillance items.[1]

I. The Proposed Interpretation of "Intrusion Software" Inappropriately Fails to Exclude Software for Defensive Activities

The interpretation of "intrusion software" put forward by BIS is overly broad and all-encompassing and fails to make any distinction between software employed for malicious, offensive activities on the one hand and software employed for purely defensive, protective activities on the other.[2] The Proposed Rule would control systems, equipment, components (4A005) and software (4D004) that are specially designed or modified for the generation, operation, or delivery of, or communication with, "intrusion software". The Proposed Rule also would control technology (4E001.a) if required for 4A005, 4D004.a (if required for 4A005 or 4D004) and if required for 4E001.c. The manner in which software meeting the characteristics of "intrusion software" is employed directly implicates the impact of the software on cybersecurity and so should play a central role in determining the export controls associated with the software.

[1] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items, 80 Fed. Reg. 28,853 (May 20, 2015) ("Cybersecurity Proposal").

[2] Cybersecurity Proposal at 28,858.

BIS has indicated that:

> some penetration testing products marketed as defensive products meet the technical description of such command and delivery platforms in the new control list entries. . . . **It is BIS's understanding that there is no technical basis to distinguish defensive products from offensive products (i.e., a defensive product may be used offensively)**.[3]

BIS has failed to establish that there is in fact no technical basis on which to distinguish defensive products from offensive products. Such distinctions are possible and more work is needed to identify technical distinctions.

A vehicle to help address the absence of technical differentiators could be a working group of technical experts representing both industry and government. The task of this working group would be to identify the technical differences between "defensive" and "offensive" cybersecurity measures. For example, the working group could provide BIS with technical details pertaining to technology and software that destroys, renders unusable, or substantially harms an information system or data on an information system which in turn will enable BIS to set appropriate controls that do not inadvertently subject exporters to burdensome and onerous licensing requirements in order to conduct day-to-day business. Distinguishing between offensive and defensive activities will enable BIS to set appropriate controls that do not inadvertently subject SIA members to onerous and unnecessary licensing requirements.

Operational or use distinctions between offensive and defensive activities are readily available and can effectively separate cybersecurity activities that pose national security risks from those that do not. Indeed, such distinctions are made in several pieces of legislation pending in the U.S. Congress. The Cybersecurity Information Sharing Act of 2015 (S.754) would permit private entities to monitor, and operate defensive measures to detect, prevent, or mitigate cybersecurity threats or security vulnerabilities on their own information systems and allow entities to share and receive indicators and defensive measures with other entities or the federal government. The legislation defines a "defensive measure" to be:

> an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability . . . {exclusive of a} measure that destroys, renders unusable, or substantially harms an information system or data on an information system not belonging to -- (i) the private entity operating the measure; or (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.[4]

The Protecting Cyber Networks Act (H.R. 1560), which passed the House of Representatives on April 22, 2015 by a vote of 307-116, and the National Cybersecurity Protection Advancement

[3] Intrusion and Surveillance Items FAQs, available at https://www.bis.doc.gov/index.php/licensing/embassy-faq#subcat200 (emphasis added).

[4] S.754, Section 5.

Act of 2015 (H.R. 1731), which passed the House on April 23, 2015 by a vote of 355-63, both also utilize the term "defensive measure."

Similar distinctions should be utilized by BIS so that software employed for defensive measures are not controlled as "intrusion software." Companies today perform vulnerability assessment using software that may fall within the proposed interpretation of "intrusion software," but should not be controlled as it is employed for purely defensive activities -- for example, the delivery of open source framework tests involving work on active rootkits and malware that is essential research to test threat mitigation. In addition, commercially available IT system vulnerability software products can perform intrusive checks, but are not specially designed for exploitation. To be able to detect and remediate vulnerabilities, companies must have the ability to exercise such software.

SIA members also may use third parties for penetration testing who use other software meeting the proposed interpretation of "intrusion software," and for purposes of testing, those third parties may use such software against their locations outside the US. This type of "white hat" vulnerability scanning or testing should not be impeded by these restrictions.

I. Certain "Intrusion Software" Should Not Be Subject to Control

All software meeting the broad parameters of "intrusion software" is captured by the proposed interpretation, regardless of the type or character of software or its availability. Mass-market software and open source software should not be subject to additional export controls even if they meet certain parameters associated with "intrusion software." Indeed, SIA understands that the Wassenaar Group discussions held in 2013 had not intended to treat mass-market software or open source software as cybersecurity software warranting stringent export control.

The interpretation of the term "intrusion software" should be narrowed to include only software that is proprietary, not generally available, and specially designed for offensive activities. Legitimate network penetration testing products and technologies, which may have been developed in the process of defending against attacks perpetrated using "intrusion software" should not be included. Accordingly, ECCN 4D004 should not include general purpose network penetration testing products.

The majority of current security research and development ("R&D") projects are cross-border, international efforts leveraging resources in countries across the world to provide robust and timely analysis and remediation. Such R&D efforts would be hampered significantly if software employed for defensive activities are not excluded from the interpretation of "intrusion software," meaning that the ability of SIA member companies to perform security testing and vulnerability analysis would be severely constrained.

II. If the Interpretation of "Intrusion Software" is Not Narrowed and Appropriate Exclusions Provided, A New License Exception Should Be Created to Cover Non-Threatening Exports of Such Software

If BIS chooses to maintain the proposed interpretation of "intrusion software," BIS should modify EAR section 740 to include a new self-executing license exception (License

Exception "CYB") pertaining to hardware, software and technology falling within ECCNs 4A005, 4D004 and 4E001 used in a particular manner.

Specifically, the following types of exports of items within ECCNs 4A005, 4D004 and 4E001 should be included within the new license exception:

1. Intra-company transfers

   Companies frequently maintain information technology ("IT") staff in several different countries and seamless interaction between those IT staff is required for efficient operation of the company. Intra-company transfers of intrusion and surveillance items and technology pertain only to the defense of corporate networks and so should not be subject to licensing requirements. Exports and deemed exports of "intrusion software" items should enjoy exemption from controls similar to those applying to intra-company transfers of encryption items set forth in License Exception ENC [Section 740.17(a)(2) of the EAR].

2. Exchange of Security Vulnerability Information

   Many companies choose not to publish or otherwise make publicly available information concerning security vulnerabilities or the techniques they are using to safeguard their own and their customers' products and networks. Nevertheless, they need to share information with respect to such vulnerabilities and techniques between and among their foreign subsidiaries, foreign national employees, and even with other companies and entities facing similar issues. Indeed, Executive Order 13,691 articulates such an information sharing requirement. The urgent need for this kind of collaboration is particularly acute where there is an ongoing attack.

3. Exports to be Used for Purely Defensive Activities

   As indicated above, it is possible to distinguish between "defensive measures" and "offensive measures." Any export associated exclusively with the former actually enhances, rather than harms, cybersecurity and so should not be of concern to the U.S. government. Any such export should not be licensable.[5]

In order to avoid a massive escalation of license applications and/or a counter-productive reduction in defensive cybersecurity measures implemented by U.S. companies, BIS should, at a minimum, create a new license exception covering such exports.

Without the ability to transfer and use these tools freely at their worldwide sites, SIA member companies may have to apply to BIS for thousands of export licenses just to support

[5] There are several examples within the EAR of use-based exceptions. Among those are (1) Regional Stability (RS) controls apply to Microwave "Monolithic Integrated Circuits" (MMIC) power amplifiers in 3A001.b.2 and discrete microwave transistors in 3A001.b.3, except those 3A001.b.2 and b.3 items being exported or reexported for use in civil telecommunications applications; (2) 3A001.a.2 does not apply to integrated circuits for civil automobile or railway train applications; (3) the inclusion of human rights considerations in licensing policy within EAR Part 742; and (4) end use and end user prohibitions within EAR Part 744.

daily security and vulnerability analysis activities. This would result in thousands of work hours for BIS and exporters, work stoppages worldwide, and increased security threats for customers while exporters wait for license processing.

III. Conclusion

As drafted, the proposed interpretation of "intrusion software" is overly-broad and imposes license requirements that are unnecessarily restrictive, significantly increasing compliance burdens on SIA members. If either that interpretation is not revised or the licensing requirements are not modified, SIA members may be required to obtain a large number of additional export licenses for products and services that are used for overwhelmingly legitimate purposes.

Moreover, if implemented as drafted, the proposed rule would impede the ability of SIA members to protect their own networks and their customers' data – undermining cybersecurity rather than enhancing it. To gain a better understanding of the potential impacts of the proposed rule, BIS should engage directly with industry and establish a working group composed of technical experts from government and industry to systematically address the technology differences between offensive and defensive cybersecurity items.

At a minimum, if BIS chooses to maintain the proposed interpretation of "intrusion software," BIS should modify EAR section 740 to include a new self-executing license exception (License Exception "CYB") pertaining to hardware, software and technology falling within ECCNs 4A005, 4D004 and 4E001 used in a particular manner.

The Proposed Rule implicates complex technical and policy issues. SIA urges BIS to pause its current push to issue a final rule, and instead, to take the additional time needed to fundamentally reconsider the proper approach to these controls. Among other steps, BIS should convene technical workshops for input and insight from industry and the security community. After such fact-gathering, BIS should issue a new proposed rule that focuses on a narrower set of items and avoids imposing undue compliance burdens on legitimate cybersecurity efforts.

* * * * *

SIA appreciates the opportunity to comment on the Proposed Revisions and looks forward to continuing its cooperation with the U.S. Government on export control reform. Please feel free to contact the undersigned or Joe Pasetti, Director of Government Affairs at SIA, if you have questions regarding these comments.

Cynthia Johnson
Co-Chair, SIA Export Control Committee

Mario R. Palacios
Co-Chair, SIA Export Control Committee