July 20, 2015 -

Kevin Wolf
Assistant Secretary of Commerce for Export Administration
U.S. Department of Commerce

Hillary Hess
Director, Regulatory Policy Division
U.S. Department of Commerce

Catherine Wheeler
Director, Information Technology Controls Division
U.S. Department of Commerce

Re: Comments on Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)

Dear Assistant Secretary Wolf, Director Hess, and Director Wheeler:

On behalf of BSA | The Software Alliance ("BSA"),[1] we write to express the significant concerns of BSA members regarding the proposed rule, with request for comments, issued by the Commerce Department, Bureau of Industry and Security ("BIS") in the *Federal Register* on May 20, 2015 (the "Proposed Rule").

The Proposed Rule implicates complex technical and policy issues. BSA urges BIS to pause its current push to issue a final rule, and instead, take the additional time needed to fundamentally consider the proper scope and 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 activities and avoids imposing undue compliance burdens on legitimate cybersecurity efforts. Once those consultations are completed, BIS should issue a second Notice of Proposed Rulemaking so that the cybersecurity community has the opportunity to review and provide comments on the revised rule.

[1] BSA's members include: Adobe, Altium, Apple, ANSYS, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, Datastax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

If implemented as currently drafted, the Proposed Rule would seriously impair the ability of BSA members to identify and fix security vulnerabilities, while requiring thousands of export licenses. The net effect may well be to diminish security for individuals and enterprises because the sheer volume of activities covered under the Proposed Rule would impose unreasonable burdens on the processing capabilities of BSA member companies as well as BIS. As currently drafted, any intended benefits of the Proposed Rule would be overwhelmed by the untenable burdens that it would place on industry and BIS.

Most importantly, we believe the Proposed Rule would hamper the efforts of cybersecurity professionals to protect our nation's critical networks and infrastructure against malicious intrusion by imposing time delays and restricting the use of the best available tools to maintain security, while doing little to impede malicious hackers from obtaining and using tools for cyber intrusions. The Proposed Rule will likely undermine cybersecurity innovation as security researchers and companies alike will be required to seek approval for a broad range of work in a profession that demands its participants move in "Internet time." The Proposed Rule fails to appreciate the global nature of the security community and the important need for international collaboration, within a company and in the security research community. An inflexible regime that is based on nationality means that systems that need protection in real-time are not afforded the best protection available because of the need for licensing and approval.

I. The Overbroad Scope of the Proposed Rule Would Negatively Affect Cybersecurity

BSA understands that the original intent for these controls, when proposed for the Wassenaar Arrangement, was to restrict the export of sophisticated surveillance systems — such as those developed and sold by FinFisher and Hacking Team — to authoritarian governments, which reportedly have used these systems to spy on or otherwise repress political dissidents and other citizens.[2] BSA agrees that such systems, which permit the targeting and monitoring of an individual's phone calls, emails, and other communications, are appropriate items for tight export controls, implemented by the United States, the European Union, and other Wassenaar members.

By contrast, the scope of the Wassenaar controls as proposed for implementation in the Export Administration Regulations ("EAR") by BIS, would apply to a far broader range of items and activities. For example:

- *Technology Controls*. Export Control Classification Number ("ECCN") 4E001.c would control "technology" "required" for the "development" of "intrusion software." Because this ECCN entry lacks specific performance levels, much of the technology related to the development of intrusion software likely would qualify as "peculiarly responsible for

[2] *See, e.g.*, Bill Marczak, Written Evidence to the UK Parliament, *Export of British-Made Spyware Targeting Bahraini Activists* (Nov. 19, 2012), *available at* http://www.publications.parliament.uk/pa/cm201314/cmselect/cmfaff/88/88vw43.htm; Response of the UK Secretary of State for Business Innovation and Skills, *Export Controls for Surveillance Equipment - Proposed JR* (Aug. 8, 2012), *available at* https://web.archive.org/web/20140816043658/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_08_08_response_from_tsol.pdf.

achieving or exceeding the controlled . . . characteristics or functions" of "intrusion software," and therefore would be considered "required" for its development. As a result this ECCN would describe an exceedingly large range of technologies, with virtually all exports and re-exports of such technology requiring an export license.

- *Software Controls*. Similarly, the proposed software controls in ECCN 4D004 attempt to limit their scope by only applying to software "specially designed" or modified for the generation, operation or delivery of, or communication with intrusion software, rather than intrusion software itself. However, BSA members report that all intrusion software that is developed for defensive/security purposes needs to be generated, delivered, and communicated with in the process of testing (and fixing) network and software security vulnerabilities. As such, BSA members report that they frequently develop and export software that would be controlled under ECCN 4D004 (as well as ECCN 4D001), both manually and through auto-code generation.

BSA appreciates the efforts that BIS has made to clarify the intended scope of the Proposed Rule, including the scope of these ECCNs, in a series of responses to Frequently Asked Questions ("FAQs") on the BIS website. However, these FAQs are not reflected directly in the language of the Proposed Rule, and do not have the force of law. More importantly, even taking these FAQs into account, BSA members report that technology and software covered by these ECCNs are frequently generated by BSA members in the course of efforts to identify and fix network, software, and other security vulnerabilities, including critical cybersecurity work to protect our nation's IT infrastructure. Because of the global nature of defensive security activities, and the wide involvement of security professionals of many nationalities, these activities require exports and re-exports to intra-company and third-party security teams in European and other countries, as well as "deemed exports" to non-U.S. nationals (lawfully working in the U.S.) and "deemed re-exports" to dual and third-country nationals lawfully working in non-U.S. countries. Moreover, these deemed exports and re-exports must occur globally and within minutes, given that vulnerabilities or threats may require tooling, software, and expertise to move as quickly as the threat.

II. The Proposed Rule Would Result in Thousands of Export License Applications

The burden of complying with the Proposed Rule would be substantial. As drafted, the rule would require licenses for virtually all exports, re-exports, and deemed exports of an overly-broad set of controlled items. Some BSA members have projected that, if the Proposed Rule is adopted, their individual companies would likely be required to obtain thousands of export and/or deemed export licenses. The number of licenses required across all BSA member companies would be much larger, and the projected number of activities and tools subject to licensing controls in the software and IT industries would be staggering. It would bring development and testing to a standstill, as the backlog of licensing requests would quickly balloon to an unmanageable level. This volume is unmanageable for even the largest companies' Trade Compliance departments, and even more importantly, BIS does not have nearly enough capacity to process these license applications.

It is also worth noting that many in the security researcher community lack the resources necessary to comply with the Proposed Rule. Much of the cutting edge work in the

cybersecurity field is performed by sole practitioners, small businesses, and academics. These entities are unaccustomed to the complexities of the export licensing process, and the delays and costs of complying with the Proposed Rule will significantly undermine their ability to participate in the cybersecurity ecosystem. Because many enterprises, including BSA members and governments, rely on their contributions, the impact on the security community will be widespread.

The Proposed Rule will make it exceedingly difficult for industry to identify and segregate controlled from non-controlled technology in the context of ongoing cybersecurity efforts; as such, industry will be forced to be over-inclusive when identifying controlled technology. Furthermore, an exporter would only need to anticipate sharing a single piece of controlled technical data with a foreign national for the export or deemed export licensing requirement to apply. The broad scope of the controls, and the ambiguities that remain even after multiple issuances of FAQs and answers, thus contributes to the massive projected licensing volume that would be created by the Proposed Rule.

The licensing burden results not only from the overbroad scope of the Proposed Rule, but also because the Proposed Rule does not offer any eligibility for license exceptions. For example, the Proposed Rule does not authorize mass-market software exports under License Exception TSU. The Proposed Rule likewise would not authorize exports of software or technology with a written assurance and appropriate compliance measures under License Exception TSR. License Exception ENC also would not be available for cybersecurity items that perform encryption.

It is important that BIS create new license exception(s) to enable legitimate and critical cybersecurity activities, such as intra-company transfers or transfers with third-party partners for security research activities. Such license exceptions are entirely consistent with U.S. participation in the Wassenaar Arrangement. The Wassenaar Arrangement is a forum for member states to agree on *what* is controlled. As explicitly stated in the Wassenaar *Initial Elements*, the decision on *how* to control the export of a controlled item is left to "national discretion."[3] Indeed, the European Union has already implemented the Wassenaar controls,[4] including the availability of general licenses for certain exports (and subject to compliance with certain additional requirements).

BIS should also reconsider the "policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities." Because most, if not all, end point security products contain some degree of rootkit functionality, a presumption of license denial will impede the ability of cybersecurity professionals to use and exchange a broad range of products and tools that are critical to protecting networks from intrusion. Restricting the exchange of items containing zero-day vulnerabilities and associated exploit capabilities will have a similar effect. Cybersecurity professionals engage in penetration testing for purposes of identifying and remediating network vulnerabilities and exploits. The tools used in penetration testing exercises

[3] *See* Wassenaar Arrangement, *Initial Elements*, Section II.3, *available at* http://www.wassenaar.org/guidelines/docs/5%20-%20Initial%20Elements.pdf.

[4] *See* Regulation (EU) No 1382/2014 (effective as of Dec. 31, 2014).

make use of zero-day vulnerabilities and then help to develop exploits to assess those vulnerabilities. The research and software engineering necessary to remediate those exploits is conducted in hours and is international in scope. To effectively close those network vulnerabilities, companies must be able to share freely and in real time. The inability to freely share the vulnerabilities and exploits that the penetration testing tools find, due to their zero-day exploit capabilities, will severely impact the ability to create safe products and ensure a secure network and IT environment.

III. BIS Should Fundamentally Rethink the Approach to these Controls and Issue a Second Proposed Rule

BSA recognizes that the goal of the Proposed Rule is to protect human rights by preventing rogue actors from undermining cybersecurity. However, by imposing enormously burdensome requirements on fundamental network security tools and practices, the Proposed Rule is likely to have the opposite effect. Securing systems and individuals against exploits, vulnerabilities, intrusions, and threats requires real-time testing and remediation actions. Such efforts must occur immediately upon the detection of a vulnerability or intrusion. As drafted, the Proposed Rule would impose burdens that will inevitably delay testing and remediation, and thus diminish security in a very real way. Both product development and security response will be stymied, as approval will be needed at each step of the process. Such an outcome would be at odds with the Obama Administration's broader cybersecurity policy, which recognizes 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."[5]

Given the complexity of the technical and policy issues raised by the Proposed Rule, BSA urges BIS, along with its inter-agency partners, to pause any current rush to issue a final rule. BIS should take the time to fundamentally rethink the approach taken to these controls -- i.e., whether to revisit the scope of the controls at Wassenaar; to issue Technical Notes, definitions, lists of excluded items within ECCN entries; or other options for appropriately drawing the scope of these controls. This also could include BIS hosting technical seminars or workshops with industry and the security community.

In the process of this engagement, BIS may identify novel approaches -- which satisfy the needs of both the U.S. Government, industry, and other organizations -- to regulation in this complex area. For example, as BIS did with encryption exports, and as implemented by the EU, there may be a registration-based approach for cybersecurity items that avoids the need for individual licensing. Alternatively, there may be end-user or end-use-based controls that more effectively control the sensitive activities of interest to the U.S. Government, without over-controlling non-sensitive, security *enhancing* activities. Such an approach could 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

[5] Executive Order 13691.

an information system. A use-based focus could help to ensure that the export control licensing requirements are not undermining the time sensitive efforts of cybersecurity professionals. However it is constructed, the final rule should be minimally invasive and maximize the ability of the security community to innovate and respond to threats and global challenges.

Once this work is complete, BIS would be in a position to issue a second proposed rule, as has been done with other complex Export Control Reform rulemakings. This second proposed rule should clearly describe the (much narrower) scope of controlled items, without reliance on FAQs on the BIS website (which do not have the force of law) and provide an opportunity for further commentary as needed.

BSA and its members welcome the opportunity to engage further with BIS, and all other interested departments and agencies, on these complex technical and policy issues.