Internet Association

INTERNET ASSOCIATION COMMENTS ON BIS IMPLEMENTATION OF THE WASSENAAR ARRANGEMENT 2013 PLENARY AGREEMENTS ON INTRUSION AND SURVEILLANCE ITEMS

1. Introduction

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies and their global community of users.[1] It is dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Network security is of paramount importance to our member companies. They work tirelessly to defend their networks and their users' data from unlawful intrusions. Public policies that undermine the ability of security researchers to protect networks – whether by design or by default – are therefore highly relevant and important to us.

The members of the Internet Association would like to thank the Bureau of Industry and Security (BIS) for providing an open comment period regarding proposed changes to the Export Administration Regulations (EAR) implementing the Wassenaar Arrangement 2013 Plenary Agreements Implementation on Intrusion and Surveillance Items. We applaud BIS officials for requesting input to better understand how companies approach security and how this rule may negatively impact those capabilities.

Implementation of the Wassenaar Arrangement in the intrusion software space is an important topic with a number of complex and potentially competing interests. The recent compromise at Hacking Team in Italy puts this complexity in stark focus. While Italy had implemented the provisions of the Wassenaar Arrangement in its export laws, a company in Italy was actively selling and supporting intrusion software to foreign governments in the exact way that the arrangement was designed to prevent.

It is clear to us that BIS is trying to put in place rules with the right intentions. However, after reviewing the proposed rules, the BIS frequently asked questions, and summaries of conference calls held by BIS, the Internet Association believes that the rules in their current form could have a negative impact on our ability to defend our networks from attackers.

Before describing our concerns with the proposed rules and our recommendations, it is important to provide some background on the various methods our member companies use to improve the security of our own systems. By describing our general approach to security, we believe we can help BIS develop a better understanding of a complex and highly specialized discipline.

[1] The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, IAC, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Pinterest, Practice Fusion, Rackspace, reddit, salesforce.com, Sidecar, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits and Zynga.

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

2. How Internet Association Members Assess Security

In the broadest sense, approaches for assessing security of systems can be placed in two categories: process-focused assessments and technology-focused assessments. Process-focused assessments evaluate the **implementation** of security controls and their supporting processes by determining if they are in place and operating effectively. These are often non-technical assessments against a recognized standard such as the Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (aka SOC2), International Organization for Standardization 27001/2, or various National Institute of Standard and Technology (NIST) frameworks. These assessments determine whether controls are operating as expected based on their design.

Technology-focused assessments evaluate the **effectiveness** of controls, often by simulating the same approach an attacker takes to break into a network or systems. These assessments can take a number of forms including, but not limited to:

- *Internal/external vulnerability scanning*: where a security practitioner uses automated tools to identify potential vulnerabilities based on non-intrusive signatures. These scans are generally focused at the infrastructure layer (e.g. the operating system and common network services such as web server software and database software).
- *Internal/external network penetration testing*: where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities and attempt to exploit them to gain unauthorized access. As with internal/external vulnerability scanning, these assessments are often focused at the infrastructure layer.
- *Application assessments:* where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in a specific application and attempts to exploit them to gain unauthorized access. These assessments are often used to evaluate security on custom-built applications.
- *Source code reviews:* where a security practitioner uses a combination of automated and manual tools to identify vulnerabilities in the source code of a specific application. As with application assessments, these assessments are often used to evaluate security on custom-built applications, generally in combination with a broader application assessment.
- *Red team/Blue team exercises*: These exercises are the most open-ended form of security assessment and they most closely simulate a real-world scenario. During these exercises, security practitioners (called the "red team") use a combination of automated and manual tools to identify vulnerabilities across an entire environment and attempt to exploit them to gain unauthorized access. Meanwhile, other security practitioners (called the "blue team") attempt to detect the red team, investigate their activities, remove them from the environment, and exfiltrate data from the network. Throughout these exercises, the red team may, under company policy, have legitimate and legal access to data relevant to the exercise that is needed to prove its success and/or to gain additional access.
- *Bug Bounties:* where a company pays independent security researchers from outside of the company to identify and report vulnerabilities in a system, allowing the company to crowdsource the identification of vulnerabilities. The researchers who report these vulnerabilities can be from anywhere in the world.

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.Internet Association.org

While different companies may use a different combination of these assessments, most companies recognize the value provided by each type of assessment and tailor their security programs around them.

3. How Security Software Tools Support Company Assessments

Security software tools play a critical role in helping make security assessments more effective by improving security practitioners' capabilities in a number of ways, including:

- *Automation and Speed*: Many companies, especially the members of the Internet Association, have large infrastructures including hundreds of thousands of servers and hundreds of network services. There is no way to perform assessments of these large infrastructures without the automation and speed that these tools provide. Manually evaluating the susceptibility of each service, on each server, for each potential vulnerability is impossible.
- *Scale*: While related to automation and speed, scaling is important to call out individually. These tools not only let companies scale to the size of their environments but also let companies scale their talent. Using effective security tools allows a company to make a practitioner more effective by having them cover a wider breadth of systems and services. Given the difficulty in hiring talented security practitioners, scaling the ones we have is critical to supporting security in large environments.
- *Proof and Validation:* Once a practitioner finds a potential vulnerability, they achieve the best results from their efforts when they are able to validate the real risk of the vulnerability, not just the perceived risk. There is a significant difference in impact when a practitioner is able to say "this is what I was able to do" as opposed to "this is what I **may** be able to do." The best way to validate the real risk of the vulnerability is to exploit it.
- *Simulation:* As explained above under "Red team/Blue team exercises", the maximum value a security practitioner can bring is through the simulation of a real world attack. "Software" "specially designed" or modified to avoid detection by "monitoring tools," or to defeat "protective countermeasures" of a "computer or network-capable device" describes tools that attackers use every day. A practitioner cannot simulate a real attack without using these types of tools.

4. The Value of Information Sharing

In addition to conducting assessments, companies often share information about emerging threats. This allows all participating companies to benefit from the efforts of a single company and respond to these threats more quickly. This information sharing happens in a number of ways including through commercial platforms, email lists, conferences, forums, and open platforms such as ThreatExchange (https://threatexchange.fb.com/). The latter platform is hosted by Facebook, an Internet Association member, and is used by a number of other Internet Association members, including Coinbase, Etsy, Google, LinkedIn, Netflix, Pinterest, Salesforce, Twitter, Yahoo, and Yelp, with more companies in the process of onboarding. Often, the information we share includes exhaustive details of tools, techniques, and procedures (TTPs) that we have seen attackers use within our networks. Sharing this level of detail maximizes the value of these exchanges.

As information sharing among organizations has grown, the value of this information sharing has grown as well. Many companies now view this as an integral part of their ability to detect and respond to new

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.Internet Association.org

threats. In fact, the U.S. government has recognized the value of this sharing as well, with President Obama issuing Executive Order 13636, "Improving Critical Infrastructure Cybersecurity". (*See* Section 4 of the Order, stating "It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats.")

While we have seen an expansion in information sharing, the industry still has a very long way to go. Most companies are not actively sharing information or have limited information sharing capabilities. In the coming years, it is critical that we focus on doing everything we can to encourage broader information sharing (subject to appropriate privacy protections) across the industry.

5. Concerns with the Proposed BIS Rules

In light of the ways in which Internet Association member companies assess their security and the value of the threat information they share, they have a number of concerns with the proposed BIS rules:

1. **There is no intra-company exception built into the proposed rules**. As a result, companies may run afoul of the rules simply by sharing software or tools that leverage exploits for testing and validation purposes within their own teams. For example, some items controlled under the proposed rules would no longer qualify for License Exception ENC, which allows for intra-company transfers.
2. **The proposed rules are broad, ambiguous, and open to interpretation.** The ongoing discussions and clarifications are evidence of how difficult the proposed rules are to understand in their current form. To date, the clarifications have addressed specific examples or identified use cases, and have not effectively refined the broader context or scope of the proposed rules.
3. **In areas where the proposed rules are clear, they create a significant regulatory burden.** Any organization that wants to develop tools that would be controlled under the proposed rules will need to implement new or updated export control processes, which will incur additional costs and increase time to market. In addition, the proposed rules create enormously complex hurdles for individual researchers who might otherwise be able to make a meaningful impact on overall security.
4. **The proposed rules would have a chilling effect on information sharing and collaboration.** Companies and researchers might elect not to share information, even if permitted by the proposed rules, due to the difficulty in understanding their restrictions. This chilling effect will be felt most strongly by independent researchers or small security companies who may lack the resources or legal support to understand and comply with the proposed rules. The ambiguity of the proposed rules only adds to this chilling effect.
5. **The proposed rules would limit a company's ability to employ non-U.S. resources in security-related activities.** Restrictions on information sharing within a company would limit the ability of companies to attract and retain well-qualified non-U.S. employees, whether in the U.S. or elsewhere, in security-related roles by requiring companies to assess citizenship and nationality and obtain export licenses in order for these employees to access controlled technology and source code. This problem would be most salient in the use of cross-border red/blue teams, but it would also arise even if entirely U.S.-based teams were used, due to the operation of BIS' long-standing "deemed export" rule. In order to avoid these costs and added

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

layers of complexity, companies might have to forgo hiring the best and brightest security experts, ultimately harming their cybersecurity.

6. **Similar rules have not worked in the past.** In the technology space, the existing rules around export of encryption technology have done little to limit the proliferation of the technology, which has resulted in a series of revisions to BIS encryption rules as the government attempted to keep pace with rapid developments in the marketplace. The proposed rules appear to be taking the same approach to a similar problem, rather than rethinking this unsuccessful approach and developing a new model to address the proliferation of intrusion and surveillance items.

6. How the BIS Rules would Impact Companies' Ability to Improve Security

Our analysis of the proposed rules has identified a number of ways in which they could, as currently drafted, negatively impact our member companies' ability to improve their own security. Provided below are some real world scenarios that illustrate this negative impact.

Impact on Security Assessments

The proposed rules would have the most direct impact on red team/blue team exercises. These assessments simulate real-world attacks by using the same TTPs that attackers use, actively compromising systems, and exfiltrating data to test defenses. The red and blue teams could be located in multiple countries. The proposed rules would cripple our ability to perform red team exercises using non-U.S. resources because we might not be able to perform exfiltration of company-owned data from company-owned systems without first obtaining an export license. This would hinder our ability to rapidly test systems in response to the discovery of a new vulnerability. Likewise, the effectiveness of blue team exercises may be limited by our inability to share certain information and tools internally with non-U.S. resources without first obtaining an export license.

Impact on Security Tools

The most obvious impact on security tools from the proposed rules will be increased cost. Commercial companies that develop tools affected by these proposed rules will need to increase the cost of their tools to offset the additional cost of the regulatory burdens they impose. Since there is no intra-company exception in the proposed rules, if any of these companies have engineering resources based in locations to which they cannot export their own software without first obtaining an export license, they may have to relocate engineering positions to new and potentially more expensive locations. Many of these costs will be passed on to their customers in the form of increased prices for purchasing licenses. In addition, consulting firms that use similar tools will pass on this cost to their clients in the form of increased consulting fees for security consulting engagements.

There is also the potential for decreased variety and capability of available security tools. Increased cost and reduced speed to market for these tools may force commercial vendors to rethink their product portfolios to reduce their regulatory burdens. In addition, obtaining export licenses for items controlled by the proposed rules will increase the time required to release new capabilities in these tools. These delays could prove harmful, given the race to fix vulnerabilities once they are known to the public. Restrictions on the export of these tools to certain destinations could also hinder efforts to

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

mitigate security risks, potentially undermining the policy goals of the proposed rules by creating a new class of "soft" targets.

Impact on Information Sharing

The proposed rules will negatively impact both inter- and intra-company information sharing. The proposed rules make inter-company information sharing far more complex and much less effective. To avoid exporting controlled items, companies will need to determine the location and nationality of any company or individual with which they want to share information as well as determine which information is controlled and cannot be shared. Additionally, while it may be possible to determine in advance the companies or individuals with which a company wishes to share information, by their very nature the information or tools to be shared cannot be determined in advance, because the threat cannot be determined in advance. Thus, proactive steps to establish information sharing channels before a crisis occurs are precluded by the proposed rules. Given the need for growth of inter-company information sharing, any regulations that discourage information sharing are cause for significant concern.

For intra-company information sharing, the proposed rules make it nearly impossible for our U.S.-based incident response teams to share fully detailed threat information with company security operations center (SOC) personnel outside of the U.S. Sending security or testing tools related to these new threats may constitute an export requiring a license, even if it is only intended for defensive purposes. For example, if a U.S.-based incident response team discovers details on a new exploit and exfiltration software being used against its systems, it may not be able to send needed tools to incident response teams in Israel without first obtaining an export license. If the U.S.-based team applies for a license, critical systems may remain vulnerable while waiting for BIS to process the application.

Impact on Bug Bounties

One of the pieces of technical information that often comes from bug bounty reports is proof of concept software or tools that can be leveraged to validate the vulnerability. This essential technical information may constitute tools that are covered under the new rules. For example, when a researcher provides us (or we provide a software vendor) with a proof-of-concept exploit and additional technical data that outlines the underlying issue, steps of exploitation, and how the vulnerability might be used in a real attack, we are creating tools covered by these rules, even though our explicit intent is to help improve defenses. Without this complete, accurate, and full picture of a vulnerability, we cannot begin to secure our systems and software. Many of the vulnerabilities we receive are highly complex and difficult to reproduce. Thus, a usable bug bounty report might not just require information about the vulnerability, it might require the provision of software "specially designed" for the generation, operation or delivery of, or communication with "intrusion software" in order to demonstrate how a vulnerability could be exploited by an attacker. If we do not receive such tools, we may be unable to reproduce the vulnerability or validate that a designed patch actually addresses it.

In addition to limiting the data provided in bug bounty reports, we fear that the proposed rules would have an overall chilling effect on researchers' willingness to participate in these programs, whether due to actual licensing requirements, or due to widespread misconceptions over what kinds of tools and information are controlled under the proposed rules. As recent coverage in the trade press indicates,

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

many security researchers believe that sharing information on exploits is prohibited under the proposed rules, even though BIS has repeatedly stated that this is not correct. This chilling effect would lead to a direct reduction in the effectiveness of bug bounty programs. (*See, e.g.,* "Student Claims Wassenaar Arrangement Prevents Him from Publishing Dissertation," *Ars Technica*, July 2, 2015, *available at:* http://arstechnica.com/security/2015/07/student-claims-wassenaar-agreement-prevents-him-from-publishing-dissertation/; "Arms Control Treaty Could Land Security Researchers Like Me in Jail," *Ars Technica,* May 27, 2015, *available at:* http://arstechnica.com/security/2015/05/arms-control-treaty-could-land-security-researchers-like-me-in-jail/)

How the Proposed Rules can be Improved

Since introducing the proposed rules, BIS has taken steps to clarify its position, but its interpretations of the proposed rules still remain unclear. For example, some of the FAQs appear to contain contradictions. As explained by the Electronic Frontier Foundation, "FAQ 10 clarifies that a researcher who has written a proof of concept for a vulnerability, 'code that takes advantage of the vulnerability,' would not be required to obtain a license before submitting the proof of concept to the vendor. But back up in FAQ 4, BIS told us that 'information on how to prepare the exploit for delivery' is controlled." In addition, responses during conference calls show that BIS is still working to understand this space. We applaud BIS for noting that they are still gathering information about the industry; however, we believe that regulating such a complex industry without a deep understanding of how all of its pieces fit together is a dangerous approach.

Industry's reaction to the proposed rules demonstrates that, while BIS has good intentions, the proposed rules will have a number of unintended consequences. If BIS feels that it must regulate these tools, it should write the rules as narrowly as possible and with the goal of minimizing their adverse impact on the following key items:

- Inter and intra-company information sharing;
- Legitimate research that helps identify and fix vulnerabilities in the systems, software, and networks we use every day;
- Bug bounty and other similar programs that help businesses secure their systems, software, and networks with the help of vulnerability researchers;
- The need of companies and individuals to use security software to identify vulnerabilities in their own systems, software, and networks;
- The power that comes from researchers producing detailed reports on vulnerabilities to help developers fix their software; and
- Additional costs that will be incurred by companies and individuals who want to use security software to secure their systems, software, and networks.

To help address the concerns raised in this public comment, the members of the Internet Association recommend the following steps to bring the proposed rules in line with the harm we believe they are truly meant to target (*i.e.*, illegal surveillance and exfiltration of data from a target without authorization):

1. Introducing an intra-company exception;

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

2. Focusing on exfiltration and the use of cybersecurity items for unauthorized activities, not the items' technical capabilities;
3. Maximizing clarity around acceptable uses that do not require a license;
4. Including more detailed language in the regulations' text and preamble, similar to was has been included in the FAQs;
5. Sharpening the definition of "Intrusion Detection Systems" to include technologies that are both system and network-based, in order to avoid conflating network intrusion detection systems (NIDS)/man-in-the-middle (MITM) tools with surveillance tools; and
6. Providing better and more comprehensive guidance to help individuals and organizations understand their obligations under the proposed rules.

Respectfully submitted,

Michael Beckerman
President & CEO
Internet Association

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.Internet Association.org