Rapid7 Comments for the Bureau of Industry and Security's Proposed Rule Implementing the Wassenaar Arrangement 2013 Plenary Agreements Regarding Intrusion and Surveillance Items

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

RE: Comments of Rapid7, Inc. Regarding the Bureau of Industry and Security's Proposed Rule Implementing the Wassenaar Arrangement 2013 Plenary Agreements Regarding Intrusion and Surveillance Items (80 Fed. Reg. 28853, May 20, 2015)

Ref: RIN 0694-AG49

Dear Sir/Madame:

Rapid7, Inc. ("Rapid7" or the "Company") submits these remarks in response to the request from the Bureau of Industry and Security ("BIS") for comments regarding the proposed rule implementing the agreements reached during the Wassenaar Arrangement's 2013 Plenary meeting (hereinafter the "Proposed Rule").

We appreciate the opportunity afforded by BIS to review the Proposed Rule and to provide comments prior to its implementation. As explained in more detail below, as a custodian and exporter of a security testing platform that would be subject to restrictive licensing requirements under the Proposed Rule, we are deeply concerned that the ultimate impact of the Proposed Rule would be to undermine (rather than enhance) cybersecurity. Specifically, we believe that the Proposed Rule would have a chilling effect on cybersecurity-related research and development efforts and make it harder for security professionals to access and deploy cutting edge tools within their organizations. Over time, we believe that the cumulative impact of the proposed controls would be to erode the effectiveness of security testing products and to impede their legitimate use. We urge BIS to reconsider the Proposed Rule in light of our comments below, and the comments provided by other interested parties. Due to the significant potential impact of the Proposed Rule on a vital part of the cybersecurity industry, we respectfully request that BIS issue another round of proposed controls before implementing a final rule.

Background

Security professionals depend on a mix of open source and commercial tools to assess their organization's security and to identify and mitigate vulnerabilities before an attack can occur. In order to be effective, these tools must mimic the tactics and capabilities of would-be attackers, including the execution of known exploits; circumvention of anti-virus and firewall; and use of the precise techniques that real attacks use to break passwords and exfiltrate data. Although some of these tools can be considered intrusion software, they are designed with the goal of improving security. In fact, certain regulated organizations are affirmatively required to conduct periodic penetration testing using these tools to ensure that they are protected against attack.[1]

Rapid7's cybersecurity data and analytics software and services help organizations reduce the risk of security breaches, detect and respond to attacks, and build effective cybersecurity programs. Security begins with identifying all network vulnerabilities that expose organizations to attack, and systematically reducing that exposure. Rapid7's Metasploit products and similar security testing solutions help organizations identify weak points in their IT environment, understand the potential impact of an attack, and mitigate the threat. Such mitigation may include deployment a patch if one is available, removing IT assets from a network, or separating databases from other parts of the network to make it harder for attackers to reach them. In instances where patches are not available, identifying and implementing alternative measures becomes even more critical.

The open source Metasploit Framework is a leading penetration testing platform that was downloaded over 200,000 times in 2014 by users across a range of industries and geographies. This technology is developed in conjunction with the wider information security community and is a critical component of many security toolkits. Rapid7 is the custodian of the Framework and employs a dedicated team of engineers who vet contributions to the Framework to ensure that such contributions do not include back-doors or other mechanisms that could make a user of the Framework vulnerable to an attack.

Rapid7 develops proprietary software based on the open source Metasploit Framework. This software includes the same attacks as the open source code, but provides additional value through automation, integration, reporting, and ease-of-use. The flagship product, Metasploit Pro, is used by security consultants and cybersecurity teams to perform security audits and penetration tests. The intrusion functionality provided by Rapid7's proprietary software is identical to the capabilities of the open source framework, which is available to the public through GitHub.com and similar distribution points for open source products.

The Proposed Rule would greatly increase the licensing burden on proprietary versions of Metasploit

Rapid7 receives hundreds of inquiries daily from individuals and entities outside the United States seeking to either purchase a Metasploit product, or to access a free or trial version of the software.

Proprietary versions of Metasploit are subject to export restrictions under the Export Administration Regulations ("EAR") and currently require a specific license for export to government end-users outside the United States and Canada. Rapid7 personnel manually screen all incoming product requests to determine whether an export license is required. Currently, Rapid7 submits approximately 10 export license applications per week to BIS. Under the Proposed Rule, Rapid7 would have to apply for licenses for all Metasploit exports, not only exports to government end-users. As a result, Rapid7 anticipates that the number of license applications would increase ten-fold to approximately 100 export license applications per week. Such an increase would require a significant investment by the Company to prepare the license applications, make further growth of the commercial product virtually impossible, and ultimately result in individuals, companies and agencies being less safe from attack.

The cost of these efforts would ultimately be reflected in the price of Rapid7's products, thus making them less

[1] For example, the Payment Card Industry Data Security Standard (PCI DSS), a proprietary information security standard applicable to organizations that process major credit cards, requires subject organizations to conduct periodic penetration tests. In addition, the National Institute of Standards and Technology resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) provides that penetration testing should be done if reasonable and appropriate.

competitive internationally and less affordable and accessible to U.S. companies and agencies seeking to protect their networks, along with the information about their employees and customers. Furthermore, the Proposed Rule would put US-based security companies that manufacture penetration testing software at a competitive disadvantage to their foreign counterparts, who would not have any of the additional administrative costs associated with managing the sale of these solutions, but could easily incorporate the same exploits into their offering.

The Proposed Rule fails to distinguish between bona fide security products that are designed to prevent misuse and other tools that are prone to misuse

The Proposed Rule would place significant restrictions on exports, reexports, and transfers of penetration test platforms, and would not distinguish between products that possess characteristics and features that deter misuse, and those that do not. For example, as noted above, Metasploit products only incorporate attack methods that are publicly available. In addition, the proprietary editions of Metasploit have a number of built-in safety features intended to ensure that the product is used only for security enhancement purposes. These features include:

- a call-in function that permits Rapid7 to identify where its product is used and to ensure that it is not transferred to embargoed destinations;
- a disabling mechanism that permits Rapid7 to disable an account from receiving exploit updates if the Company determines that the product is being misused;
- the use of extensive logging within the product to ensure that all actions taken by the user can be audited and verified at a later date; and
- the use of encryption to protect the integrity of the logs.

The incorporation of the above safeguards does not interfere with the commercial editions of Metasploit's effectiveness as a security tool, but does make them less attractive to those who would use the product for malicious purposes.

By not distinguishing between products that deter misuse and those that do not, BIS is missing an opportunity to encourage developers of controlled products to incorporate features to maximize accountability and to ensure that their products are used only in legitimate security contexts. We believe that BIS should create a list of features (like those in Metasploit and other products) that, if present, would exempt a product from the proposed controls on intrusion platforms altogether, render the product eligible for favorable license exceptions, or subject the product to less stringent export licensing requirements.

Products that test for zero-day exploits and rootkits are not inherently malicious and should not be subject to a policy of denial

Rapid7 is opposed to BIS's proposed policy of denial for license applications relating to products containing "zero-day exploit" and "rootkit" capabilities. The presence of these capabilities in commercially available penetration testing products does not render such products inherently more prone to misuse. Nor do they determine the defensive or offensive nature of a product. In reality, by their very nature, these kinds of defensive security testing products must simulate offensive tools and tactics. As noted above, we believe that BIS should adopt rules that specify product characteristics that, if present, may exempt an item from the scope of the controls, or render the item eligible for license exceptions or other favorable treatment.

Organizations routinely test their networks to identify potential entry points for attackers, and understand the impact of an attack. Both zero-day exploits and rootkits play a vital role in this investigation, and so both are frequently found in defenders' toolkits – not just in use by bad actors.

Should BIS disagree and decide to consider the presence of "zero-day exploit" and "rootkit" capabilities when making licensing decisions, we believe that those terms must be explicitly defined. In our view, the terms "zero-day exploit" and "rootkit" should be defined to mean only those exploits and rootkits that are not publicly known or available.

The definitions of "zero-day exploit" and "rootkit" should not be dependent on whether or not a patch for the vulnerability is publicly available, or whether a software developer has taken steps to fix a known vulnerability. Many developers are reluctant to fix vulnerabilities even when they are known, and in other cases there may not be a patch available because the software developer is no longer in business or no longer supports the product. For these reasons, it is the public nature of the vulnerability and the exploit that should be determinative. Once the presence of a vulnerability can be tested for and identified, positive pressure can be placed on the responsible software developer to address the vulnerability and thereby enhance security. Moreover, even if there is no patch, identification of vulnerabilities allows security administrators to make choices about what products they use, how they structure their networks, and what information they put at risk.

Rapid7 submits that the following proposed definitions of "zero-day exploit" and "rootkit" provide the appropriate degree of clarity, while also distinguishing between public and non-public exploit capabilities:

- **Zero-Day Exploit:** A software tool that takes advantage of a security vulnerability that is not publicly known. Security vulnerabilities will be deemed publicly known if: (1) they are the subject of a notice that was made generally available to the public; or (2) they are being actively exploited by criminals.

- **Rootkit:** A non-public, post-exploit software tool that is primarily useful for maintaining control of a computer system without being detected, in a manner that is not authorized by the owner or system administrator of the computer system, after the computer system has been compromised.

The Proposed Rule will have a chilling effect on security research and development efforts

The Proposed Rule does not specifically address security research and vulnerability reporting activities. BIS has stated that its intent is not to interfere with "non-proprietary" research activities (i.e., research activities that are intended to lead to the public identification and reporting of vulnerabilities and exploits). Information and software that is publicly available is not subject to the EAR.

The Proposed Rule, however, would establish controls on "technology required for the development of 'intrusion software,'" which would regulate exports, reexports and transfers of technical information required for developing, testing, refining, and evaluating exploits and other forms of software meeting the proposed definition of "intrusion software." This is the type of information and technology that would be exchanged by security researchers, or conveyed to a software developer or public reporting organization when reporting an exploit.

We are concerned that ambiguities regarding the application of the proposed export licensing requirements will have a chilling effect on security research and reporting activities. Accordingly, Rapid7 respectfully submits that BIS should implement explicit and clear protections for activities relating to security research and the public reporting of exploits. Research and reporting activities are vitally important to the development of new and effective security tools.

The absence of license exceptions will make it harder for companies to deploy Metasploit and other controlled products for their own internal use

Currently, security testing products and other items that fall within the definition of controlled items are subject to encryption controls under the EAR. As such, they benefit from license exceptions that permit the distribution of products to and among foreign subsidiaries of U.S. companies for internal use, the hand carriage or temporary export of these tools outside the United States, and the release of certain software products and associated technology to foreign employees of the U.S. company and its foreign subsidiaries.[2] Under the Proposed Rule, however, exports of controlled items generally would not be eligible for license exceptions under the EAR. As a result, exports that facilitate the widespread deployment and use of security tools within an organization would be barred in the absence of an export authorization issued by BIS. This could lead to delays in the deployment of products, as well as delays responding to attacks. It could also lead to the submission of more voluntary self-disclosures to BIS as security professionals facing attacks are forced to choose between deploying a controlled product internally and waiting for the issuance of a license. Rapid7 strongly opposes any regulatory measures that would make it harder for security professionals to protect their networks.

Real-world scenarios where the rapid deployment of security tools is imperative include:

- Organizations that are high value targets are under constant attack due to the sensitive information they possess (e.g., military technology, personally identifiable information, financial data, trade secrets, etc.). Should use of a new or innovative security tool allow them to better withstand or recover from these attacks, they may not be able to wait for an export license authorizing them to deploy the software to their overseas facilities for their own use and security.

- In the merger and acquisition context, it is customary for acquirers to conduct extensive penetration testing of companies that they plan to purchase as part of the due diligence process. This is done to ensure that threats on the target's network are identified and mitigated prior to integration. In this context, there may not be a sufficient window of time to wait for an export license to test overseas facilities. Once a transaction is announced, attackers will potentially target the acquired company's network as a way into the acquirer.

- An organization on a receiving end of an extortionate threat would need to quickly ascertain the likely impact of an attack, and isolate or protect high value information.

Rapid7 respectfully submits that BIS should authorize the use of Metasploit and similarly controlled security testing platforms by U.S. companies and their foreign subsidiaries in a manner coextensive with Paragraph (a)(2) of License Exception ENC (15 C.F.R. 740.17(a)(2)). Further, we believe that security professionals should be authorized to travel outside the United States with controlled penetration test platforms as tools of trade under License Exception TMP (15 C.F.R. 740.9) or License Exception BAG (15 C.F.R. 740.14).

[2] For example, penetration testing and other cybersecurity products that utilize encryption are currently subject to export restrictions under the EAR. Paragraph (a)(2) of License Exception ENC authorizes U.S. companies to export specified encryption commodities (including associated software and technology) to any "U.S. Subsidiary." In addition, paragraph (a)(2) of License Exception ENC also authorizes the export or reexport of such items by a U.S. company and its subsidiaries to foreign nationals who are employees, contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use, including the "development" or "production" of new products.

Due to the importance of U.S. Companies to global cybersecurity, it is crucial that BIS get the implementation of these controls correct

BIS's implementation of the Wassenaar Arrangement's agreements on intrusion and surveillance items will have far reaching consequences. Because of the leadership of U.S. companies in the cybersecurity industry, the sheer number of U.S. multinational companies, and the fact that U.S. companies are often the target of cyber-attacks, the impact of BIS's implementation is likely to far outweigh that of other Wassenaar members. For this reason, BIS should not simply follow other Wassenaar members, many of which oversee export control systems that differ markedly from the U.S. in terms of scope (such as the absence of deemed export controls in many European states), resources, and enforcement.

We urge BIS to make every effort to avoid impairing the ability of U.S. companies to develop and market innovative and effective security tools. Further, BIS should seek to affirmatively facilitate (rather than regulate) the ability of U.S. multinational companies to deploy security products for their internal use. This means breaking down barriers to intra-company releases of controlled intrusion products and associated technology.

*   *   *

We appreciate the opportunity to share our views, and would be pleased to further discuss our concerns with BIS staff.

Once again, given the significant potential impact of the Proposed Rule on a vital part of the cybersecurity industry, we respectfully request that BIS publish another round of proposed controls for review and comment before implementing a final rule.

Sincerely,

Rapid7