July 20, 2015

Via email to publiccomments@bis.doc.gov

Kevin J. Wolf
Assistant Secretary for Export Administration
Regulatory Policy Division, Bureau of Industry and Security
U.S. Department of Commerce
Washington, DC 20230

Subject: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (Docket No. 150304218-5218-01; RIN 0694-AG49)

Dear Assistant Secretary Wolf:

Our organizations, which represent nearly every sector of the U.S. economy, welcome the opportunity to comment on the Bureau of Industry and Security's (BIS') proposed rule, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, released in the *Federal Register* on May 20, 2015.[1] Cybersecurity is a top policy priority of our members. The goals of the Wassenaar Arrangement (WA) are constructive, and our organizations appreciate BIS' attention to combating the proliferation of malicious and weaponized software. However, we have genuine concerns that if the proposed rule were to go into effect without substantial changes, it could harm rather than improve U.S. cybersecurity.

We do not attempt to answer each question in the May 20 notice seeking comment. However, we try to explain why our organizations believe that BIS' proposed rule is too expansive and the license requirements are overly strict. Our associations recommend that BIS narrows the breadth of cyber items that would be controlled and builds more flexibility into the rule's conditions. We believe that the United States can meet the terms of the WA without sacrificing the prudence needed to make the proposal.

Businesses would likely need to submit hundreds, perhaps thousands, of additional license applications under the requirements of BIS' proposed rule.

The number of new export licenses that U.S. companies would have to request from BIS could be staggering—ranging from hundreds to perhaps thousands—depending on the number of products in their software portfolios. Factors influencing license applications include the volume of third-party software and services that companies use in their own operations, the number of offices that they have outside of the United States and Canada (which is exempt from the proposed rule), and the number of engineers that companies employ or are in contact with who are not American citizens. Also, the burden of determining what activities require licensing would be significant for businesses' software development cycles, code in transient states, and

[1] www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

email communications housing information—all of which may be ostensibly covered under BIS' proposed rule.

Making matters more complicated, the bureau's proposed rule states that "when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled cybersecurity functionality."[2] The bureau should reconsider the mandate for applicants to hand over their source code. This is particularly important at a time when U.S. officials and industry are urging foreign governments not to compel vendors to turn over intellectual property, such as source code and other sensitive corporate data.

The rule would have negative effects on businesses' legitimate vulnerability research, audits, testing, and screening. Businesses' ability to protect their (or a client's) information systems would be thrown into question.

"Intrusion software"-related items as listed under the Wassenaar Agreement (WA) and proposed for regulation by BIS would severely restrict security vulnerability improvements and R&D undertaken by U.S. companies, academia, nonprofits, and individuals. The proposed rule would affect entities that create or operate intrusion software and any information system that "communicates with" such intrusion software.

To be sure, BIS argues that intrusion software, malware, and exploits themselves would not be controlled. For instance, in an FAQ supplement to the proposed rule, the bureau tries to distinguish between "intrusion software," which is not controlled per se, and items such as "command and control and delivery platforms," which would be controlled by U.S. export officials:

> [T]he proposed rule would not control any "intrusion software," which may also be referred to as malware or exploits. The Category 4 control entries would control the command and delivery platforms for generating, operating, delivering, and communicating with "intrusion software." It would also control the technology for developing "intrusion software," but it does not control the "intrusion software" itself. Thus, transferring or exporting exploit samples, exploit proof of concepts, or other forms of malware would not be included in the new control list entries and would not require a license under the proposed rule.[3]

What is especially challenging for our organizations to understand is that BIS, in order to comply with WA, would require businesses to make nuanced distinctions between various forms of intrusion software and the technical data for developing exploits. Such differentiations are nearly impossible to make in practice.

In addition, BIS' rule proposal would significantly restrict testing and research into cyber vulnerabilities and exploits connected to valuable internal business activities ("intra-company transfers or internal use"),[4] which are designed to strengthen their cyber defenses worldwide.

---

[2] See, for example, FAQ No. 7 via www.bis.doc.gov/index.php/policy-guidance/faqs.

[3] See FAQs Nos. 1 and 3.

[4] See FAQ No. 17.

Such limitations are troublesome to our associations. On the one hand, business initiatives meant to protect their information systems should be aided and encouraged, not restrained. On the other hand, delays in approvals for license applications would almost certainly leave critical data systems much less protected and subject to increased cyberattacks or breaches by malicious actors.

The proposed rule would spur the publication of unpatched vulnerabilities and constrain businesses' ability to defend their information systems.

The apparent goal of BIS' proposal is to reduce the production and sale of malicious and weaponized software. Strangely, the BIS proposal could have the exact opposite effect. The model that many in industry have for managing vulnerabilities is based on communicating unpublished vulnerability information to companies that can fix software problems before weaknesses are exploited. However, the proposed rule suggests forcing companies to publish vulnerabilities first—or otherwise making them publicly available—in order to conduct necessary research on exploits and transfer information in compliance with export rules.[5]

Revealing vulnerabilities before patches can be built is very disconcerting. The proposed rule would stimulate the publication of vulnerability information for which no known patches, fixes, or mitigations may be available. Instead, our organizations believe that BIS should be encouraging the discrete transfer of information about previously unknown vulnerabilities to the developers of the technology affected.

Also, the bureau's proposed regulation would impose significant constraints on the ability of multinational corporations to take cyber self-defense actions, which private entities have an inherent right to. Companies' vulnerability assessment personnel—aka red teams—use "intrusion software" to identify and track vulnerabilities in network devices and applications. Our organizations believe that the ability of companies to perform this activity across global boundaries, but within the confines of a single firm, must not be curtailed.

The BIS' proposal would advance "a policy of presumptive denial" for zero-day and rootkit capabilities, e.g., "product or system" or "delivery tool" (p. 28855).[6] Presumptive denial would greatly restrict businesses' abilities to share threat information and counter some of the most dangerous cyber vulnerabilities and exploits.

Detailed technical data on the origins of a previously unknown vulnerability—a zero-day—is also the technology that enables bad actors to exploit weaknesses in a computer system. Potentially high-risk vulnerabilities are the exact type of cyber weaknesses that companies want to find during their internal penetration testing and exercises. Such vulnerabilities are given top priority by companies to examine and mitigate or eliminate fully to render exploits useless.

Zero-days are among the most dangerous of all cyber vulnerabilities and associated exploits, and they are unknown to the broader cyber stakeholder community. Responsible companies take vigorous steps to ensure that this sensitive information never leaks to the public,

[5] See FAQ No. 5, among others.

[6] See, too, FAQ No. 22.

which conflicts with BIS' push to make cyber technology or software "publicly available."[7] Zero-day exploits have been known to cripple companies and their customers. The business community needs to be able to disseminate vulnerabilities and technical details to knowledgeable experts in their companies and trusted industry partners. Sometimes the experts will not be American or Canadian citizens.

If BIS automatically denies licenses for cyber items that have zero-day exploits, the policy could dramatically hinder a company from fixing the vulnerability, thus putting itself and its customers in jeopardy. We believe that BIS does not seek such an outcome from the proposed rule.

On a more granular level, BIS' proposed export control regime would impose severe limitations on currently lawful and smart business activities, including the following:

- The development, operation, and functionality of automated security vulnerability identification and reporting tools, application program interfaces (APIs), or backend systems that companies build into their own software products to defend their information systems.

- The speed of deployment of security patches for products impacted by intrusion software and related exploits (e.g., POODLE).

- Vendors that companies use for collecting and analyzing cybersecurity information and intelligence.

- Email accounts set up by companies to specifically receive security threat and vulnerability information from the general public.

- Software products that companies sell to provide situational awareness concerning cyber threats to their own computer systems as well as those of their customers.

- The work of security vulnerability researchers at U.S. and international universities that share threat information directly with U.S. companies (e.g., zero-day vulnerabilities) over email.

- Bug bounties and hackathon events, which are created to identify security exploits and then share that information back with the affected companies as quickly as possible.

- The types of audits that companies would be allowed to perform on third-party vendor systems and whether bugs could be reported back to them directly when discovered.

- The sharing of information between a single company's employees if someone within the United States shares technical data about security threats with a person who is not a citizen of the United States or Canada.

[7] See, for example, FAQ No. 28.

- Threat data that companies and researchers need to share in timely ways within public-private partnerships (e.g., sector-coordinating councils and information-sharing and analysis organizations).

- Information sharing linked to government contracts and protected programs. First, information that is shared with the U.S. government voluntarily (e.g., US-CERT) or as required under contracts (e.g., FISMA and FedRAMP) could be thrown into question, which would benefit neither the government nor the private contractor.

  Second, at the time of this writing, legislation is being considered in Congress for spurring the voluntary sharing of cyber threat information among multiple businesses and federal entities to improve cybersecurity. The bureau's proposed rule could undermine, albeit unintentionally, the sharing processes and safeguards (e.g., legal liability and regulations) afforded to U.S. companies under the legislation.

Big picture: Our organizations believe that BIS' proposed rule is much too broad and the license requirements are unreasonably stringent. The bureau should consider both narrowing the scope of the proposed rule (in terms of cyber items that would be swept up and controlled) and building more flexibility into the rule's requirements. We believe that the United States can thoughtfully meet the terms of the WA without sacrificing the discretion required to make the proposal achievable, especially as it relates to safeguarding legitimate enterprise cyber risk management activities.

Aside from offering the perspectives above for BIS' consideration, our organizations have further topics and questions that we respectfully ask bureau officials to please clarify:

- The proposed rule targets "technology required for the development of intrusion software" (p. 28853). Generally, to develop intrusion software for the Windows environment, you need tools such as Wintel-compatible hardware and a Windows operating system. Most companies use such tools for all their internal application development. However, an initial reading of the BIS notice could lead entities to believe that Wintel-compatible hardware and Windows operating systems would be controlled since they are required for development of intrusion software, which is not BIS' intent.

  Therefore, shouldn't the proposed rule's wording be changed to something closer to "technology required *solely* for the development of intrusion software and not used for *legitimate* purposes" (italics added for emphasis)? The WA goal, which BIS and our organizations share, is to dramatically limit the actions of bad actors while enabling businesses to conduct rightful security activities.

- Some interpret the proposed rule's language—"systems, equipment or components specially designed for the generation, operation or delivery of, or communication with, intrusion software; software specially designed or modified for the development or production of such systems, equipment or components; software specially designed for the generation, operation or delivery of, or communication with, intrusion software" (p.

28854). The word "specially" is seemingly meant to differentiate legitimate from illegitimate uses of intrusion software, but it is far from clear.

We suggest that BIS make it clear it is not talking about systems, equipment, components, and software that have legitimate purposes, even if bad actors use the same items for the purpose of invading information systems.

- BIS should better define what "communication with intrusion software" (p. 28854) means. At this point in the rule development process, it appears that nearly every software tool used to fight malicious software and intrusion software would be included. This cannot be the outcome that BIS is seeking.

- Most companies utilize some type of packet analyzer (aka packet sniffer) to monitor and capture digital traffic passing over a network so that technicians can identify malicious code. In 2013, WA agreed to add the following to their list of dual-use goods, including "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" (p. 28854).

  Does the inclusion of IP network communications, etc., mean that companies would no longer be able to move their monitoring equipment and software from location to location in their networks to fight bad actors? Requiring government's approval for such smart and basic cybersecurity practices strikes us as logistically unfeasible and detrimental to enterprise security.

- Most large multinational firms regularly undergo penetration testing to spot and remediate vulnerabilities in their computer systems. The proposed rule would impact "[s]ystems, 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" (p. 28854).

  Such language suggests that companies would have to gain licenses for nearly every test that they conduct outside the United States, since they would be moving computer equipment and software. While BIS is supposed to maintain U.S. export controls on items included on the WA's control list, the bureau is probably not intending to make it *more* difficult for businesses to defend themselves, which is what this clause suggests.

***

Our associations are committed to working with BIS officials and other policymakers to strengthen U.S. cybersecurity by advancing smart, effective, and efficient policies at home and globally. We appreciate the opportunity to comment on the bureau's proposed rule. Our members particularly appreciate the constructive outreach that they have had with BIS officials—Catherine "Randy" Wheeler, Aaron Amundson, and Anita Zinzuvadia. We urge the BIS not to rush to finalize this proposed rule, which is unworkable in its current form. The

proposed regime would tie the hands of businesses' legitimate cybersecurity activities while malicious actors simply disregard compliance.

Sincerely,

Alliance of Automobile Manufacturers
American Petroleum Institute (API)
Computer & Communications Industry Association (CCIA)
Information Technology Industry Council (ITI)
Internet Association
Financial Services Roundtable/BITS
National Foreign Trade Council
TechNet
Telecommunications Industry Association (TIA)
U.S. Chamber of Commerce