Congress of the United States
Washington, DC 20515

July 20, 2015

Catherine Wheeler
Director, Information Technology Control Division
c/o Regulatory Policy Division
Bureau of Industry and Security
Room 2099B, US Department of Commerce
14th St and Pennsylvania Ave NW
Washington, DC 20230

Re: RIN 0694–AG49 – Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Director Wheeler:

Thank you for the opportunity to comment on the Bureau of Industry and Security's proposed rulemaking RIN 0694–AG49, regarding the addition of new dual-use technologies to the Wassenaar Arrangement Annex. We write as Members of Congress with an abiding interest in national security in general and cybersecurity in particular. While we are sympathetic to BIS's goals in implementing the 2013 additions, we are deeply concerned that the regulations could unintentionally weaken our security posture.

There is no doubt that, in the wrong hands, offensive hacking tools can cause great damage. Whether it results in the exfiltration of sensitive data, as in the recent breach of the Office of Personnel Management, or the execution of malicious commands, such as those that destroyed thousands of computers at Sony Pictures Entertainment, malware has proved to be a great scourge of our digital age.

As such, there are very legitimate concerns that intrusion software developed in countries party to Wassenaar could find its way into the hands of criminal organizations or even repressive regimes. In fact, the recent dump of data from Hacking Team, an Italian security firm, bears out these fears. Leaked emails and spreadsheets strongly suggest that Hacking Team sold tools to the Ethopian government that were later used to commandeer journalists' computers so that they could be monitored. Worse, Hacking Team files indicate that the company sold its products to the government of Sudan, a country that is sanctioned by most of the international community due to its history of violence against its people.

When the Wassenaar Arrangement Plenary agreed to add intrusion software to the annex, it was exactly technologies like Hacking Team's that the members intended to regulate. Unfortunately, the agreed upon definition for intrusion software is quite broad, embracing a number of products that are solely intended for research. BIS's proposed implementation of the new definitions, while cognizant of this potential problem, serves only to exacerbate it by drawing a misguided line between offensive and defensive cyber tools. Combined with the lack of a waiver of deemed export rules, this could have a chilling effect on research, slowing the disclosure of vulnerabilities and impairing our nation's cybersecurity.

Zero-Day Vulnerabilities

Of paramount concern in the proposed rule is BIS's treatment of zero-day or rootkit capabilities within intrusion software. BIS does not define "zero-day" or "rootkit" in the NPR, which is, in itself, troubling. Our interpretation of the rule views a "zero-day" as a software vulnerability that does not yet have a patch

designed to mitigate it. We understand a "rootkit" to be intrusion software with the capability of giving its user unfettered – root – access to the underlying operating system. BIS indicates that license requests for software making use of such capabilities would be presumptively denied.

We understand that BIS's intent in including these additional terms was to delineate between offensive and defensive intrusion software. Because there are no patches for zero-days, a firm doing a penetration test to judge a client's patch management program would have no need to include a zero-day in its testing suite. However, cybersecurity risk management frameworks operate on the assumption that breaches will happen, and that a manager must therefore not rely solely on perimeter defenses. Network operators, therefore, may wish to assess how their systems respond to a wholly novel threat. Preventing the export of testing frameworks that make use of zero-days could, therefore prevent comprehensive evaluation of cybersecurity posture.

Rootkits pose a similar problem. Demonstrating a vulnerability or performing a penetration test does not always require the vulnerability to acquire root access. However, certain vulnerabilities, particularly those targeted at the operating system, are based on privilege escalation – gaining administrator access without appropriate credentials – and any related demonstration code would necessarily be considered a rootkit. Furthermore, mature cybersecurity strategies should recognize the potential for rootkit infection and employ detection measures that rely on alternate means, such as traffic analysis, to identify compromised systems. Precluding export of rootkits can thus also impact cybersecurity.

Deemed Export

We are also troubled by the implications of applying the "deemed export" regime to intrusion software, a rule that has not been adopted by European Union members in implementing the Wassenaar Arrangement. Many American companies have multinational footprints, and even those solely operating within the United States often employ foreign nationals, particularly in fields like cybersecurity that suffer from an acute talent deficit. Similarly, academic institutions around the country have a significant minority of foreign graduate students, many of whom are at the front lines of information security research.

We see two significant challenges in applying the deemed export rules to these technologies. Third parties often disclose vulnerabilities to anonymous email addresses established specifically for this purpose. A security researcher thus has no way of knowing who precisely will see the disclosure. Requiring a careful chain of custody for researchers to ensure they don't inadvertently "export" a vulnerability by sharing it with foreign national employed by a developer could easily disrupt the entire reporting ecosystem.

Furthermore, if companies or researchers are required to segregate data based on nationality or to apply for a license to share information with their own students or employees, research will suffer. Companies may be unable to share threat data with their own international affiliates, at least not in a timely manner. Because hackers can attack overseas just as easily as domestically, any weak system with access to a business's internal network represents a serious vulnerability.

As you are no doubt aware, Congress is very interested in expanding information sharing of cyber threat indicators. Two bills have already passed the House this session attempting to incentivize information sharing, and the Senate Select Committee on Intelligence has favorably reported a similar measure. We hope that the final BIS rule will further these efforts, or at the very least not hinder them.

Research Exemption

In its conversations with stakeholders, BIS has emphasized that publicly available intrusion software is not subject to export controls. Beyond the Constitutional requirements that may motivate it, this is a wise

policy that helps foment an innovative research environment. However, we are concerned that BIS is overly reliant on the public research exemption as a way for intrusion software developers to escape otherwise broad regulations.

Responsible disclosure first involves a researcher privately contacting the owner of a piece of vulnerable software. Sometimes, the vulnerability in question will be made public because the developer refuses to patch it. Sometimes, the vulnerability will be patched, and then the exploit will be incorporated into open source penetration testing software. However, there are cases when an exploit will be patched silently in an effort to avoid giving malicious actors a blueprint to flaws in a system. The BIS rule, as proposed, also does not clarify exactly when an exploit goes from being controlled to being public, which could further complicate the efforts of security researchers.

Conclusion

Part of the difficulty faced by BIS stems from the underlying language agreed upon by the Wassenaar parties. That "intrusion software" encompasses vulnerabilities at all is something that the international community may wish to revisit during future negotiations. Information systems security is still a new field, and policy tools are still being developed and calibrated.

The recent Hacking Team revelations have driven home the need for reasonable export controls on software that can be used by criminals and governments to attack citizens around the globe. While we have serious concerns about some of the provisions of the proposed rule, we do not doubt the need for it. To ensure that the rule is narrowly targeted, we strongly encourage BIS to consider issuing another draft rule for comment before finalizing the implementation.

Thank you again for the opportunity to comment on this important issue. We must also commend BIS for its extensive outreach effort – both through the Department of Commerce and the Department of Homeland Security – with stakeholders in academia and industry. If you have any questions regarding the submittal, please contact the Office of Congressman Langevin at (202) 225-2735.

Sincerely,

JAMES R. LANGEVIN
Member of Congress

DAVID SCHWEIKERT
Member of Congress

MICHAEL MCCAUL
Member of Congress

TED LIEU
Member of Congress