Statement of

Kevin J. Wolf
Assistant Secretary of Commerce for Export Administration

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

And the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

January 12, 2016

Thank you, Chairmen Hurd and Ratcliffe, and Ranking Members Kelly and Richmond.

The Wassenaar Arrangement is a 41-member export control group in which the United States participates. It was established to contribute to regional and international security and stability by promoting greater responsibility in the transfer of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations of such items. Participating States maintain a common control list of items warranting control for these reasons and seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals, and are not diverted to support such capabilities. The list of such items is developed and updated by the Participating States through consensus determinations, generally made at the end of each year.

The U.S. Department of State leads the U.S. delegation to the Wassenaar Arrangement but my agency, the Department of Commerce's Bureau of Industry and Security, is responsible for developing and administering the U.S. regulations – the Export Administration Regulations – that implement U.S. export controls for dual-use and some military items on the Wassenaar control list. Other agencies, primarily the Department of Defense, participate in developing proposed changes to the control list to submit to Wassenaar, deciding whether and which controls to agree to, and reviewing the U.S. regulations to implement controls agreed to by the member states. Commerce also has technical advisory committees composed of private sector experts who provide technical and other advice regarding proposals to the regimes.

In December 2013, Wassenaar approved new export controls on "command and delivery platforms" for "intrusion software" and related technology. Specifically, the entries in Category 4 (Computers) of the Wassenaar dual-use control list would control non-publicly available software (4.D.4.) that generates, operates, delivers, or communicates with "intrusion software." "Intrusion software" is defined as software designed to covertly gain access to a computer or other networked device and, once inside, to extract or modify data or modify the execution

path of the device to allow the execution of externally provided instructions. Related hardware and technology entries (4.A.5. and 4.E.1.c.) control systems and equipment for generating, operating, delivering, or communication with “intrusion software," and technology for developing “intrusion software.” The original proposal for these controls came from another Wassenaar member nation in 2012. Examples of the types of commercial hacking software intended to be captured by this control include those offered by Hacking Team (Italy), Gamma/Fin-Fisher (Germany), and Vupen (France).

The controls were novel in that they were the first foray by a multilateral export control community into the area of offensive cyber tools. The agreed-upon entries covering software intentionally excluded "intrusion software" itself -- that is, certain kinds of malware -- from control because of a general understanding that everyone with a computer or mobile device infected by such malware or “exploits” could become an unwitting “exporter” of it (e.g., by forwarding an infected e-mail to someone in another country). The technology entry, however, imposes controls on non-publicly available technology for the development of such software as well as on technology for the development of the controlled delivery systems.

In beginning the process of drafting the regulation to implement the control, Commerce grew concerned that, despite several exclusions set forth in the definition of “intrusion software,” the scope of the controls, particularly the technology controls, might be far broader in scope than originally understood by Commerce and its advisory committees. We particularly became concerned that the Category 4 technology control list entry in the draft regulation -- technology for the development of “intrusion software” -- could inadvertently significantly harm both U.S. government and U.S. private sector cybersecurity programs and efforts if implemented.

In order to not take an action that would inadvertently harm our nation’s ability to engage in critical cyber defense and related research work, we decided in May 2015 to take the unprecedented step of publishing these Wassenaar control list entries as a proposed rule, with a request for private sector comments, rather than as a final rule. Our hope was that the private sector comments would give us a better sense for whether the rule would have unintended impacts on our cyber defense and cyber research ecosystems. All dual-use controls have consequences and impose costs on the private sector. That is the nature of controls. This one, however, was different because the impact would be not just on the economic bottom-line of U.S. companies, but on our government’s and our nation’s ability to share efficiently and quickly the types of technology necessary to conduct cyber defense and related research.

Immediately following publication of the proposed rule, Commerce received questions from U.S. private sector and others in the U.S. Government about the intended scope of the controls. In order to ensure that comments were informed and responsive to the proposed controls set forth in the rule, Commerce published answers to a list of “frequently asked questions” on its website to address what we determined were regular queries in order to encourage more focused and more useful public comments. It was clear from these initial questions that the terminology used in the control list entries and the proposed rule were understood differently by the cybersecurity community than by the export control agencies and the Wassenaar Participating States. By the end of the 60-day comment period, Commerce

had received more than 260 comments, virtually all of them negative. Some commenters took the view that the underlying control at Wassenaar could not be implemented without causing significant harms to cybersecurity. Others made specific recommendations on ways to mitigate many of the concerns. Some praised the underlying objectives of the rule, while nonetheless proposing modifications to the scope of the proposed regulation, such as through license exceptions and definitions, to reduce the impact of unintended consequences.

The negative reactions were repeated by extensive outreach our bureau conducted with the security industry, information security and financial institutions, and government agencies that manage cybersecurity. Outreach included multiple open meetings under the auspices of Commerce's technical advisory committees and extensive discussions with cybersecurity managers in the Federal Government.

Neither the Commerce Department nor the Administration has reached a conclusion about how to respond to the public comments. We are still reviewing and considering them. Importantly, all U.S. Government agencies with expertise and equities in cyber defense research and related work are reviewing the comments and will provide input as a next step, before we make a decision on what to do about the proposed rule. As requested by your committees, I can, however, summarize the essence of the comments – reiterating that the Administration has not come to any final conclusions regarding how to respond to the comments or to the extent to which they are correct technically. The public comments, including presentations at technical advisory committee meetings during the past three months, focus on three main issues.

First, some commenters asserted that the proposed regulation's definition of "intrusion software" is too broad and, as a technical matter, fails. They assert that malware recovery tools would be caught by the entries because they interact with malware to regain control of an infected system, and some defense research tools would be caught because they analyze malware to develop new defensive products. They also assert that products that patch systems or add capabilities to programs would themselves be controlled under these entries because of the way they interact with or manipulate programs. These products are integrated with the hardware (systems, equipment, and components) and are designed to legitimately bypass or defeat protections, modify the standard execution path of software, and access data. According to the commenters, they would often thus be software for the generation, operation, delivery of or communication with "intrusion software" and caught by the new controls.

Second, other commenters contend that the proposed rule to implement the control list entries as written, based on the definition of "intrusion software," would impose a heavy and unnecessary licensing burden on legitimate transactions that contribute to cyber security. Government agencies and private sector cyber security companies routinely test their systems and networks to identify vulnerabilities and, if possible, discover existing malicious attack agents. These companies then provide their clients with threat mitigation tools and strategies. To accomplish this, they use the same tools the controls on intrusion items identify, though their use is authorized by their target. To accomplish their mission, they need to employ tools for computers or networks that have the functional specifications of the control parameters, *e.g.,* avoid detection, defeat protective countermeasures, extract data or information, modify

system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are exactly the characteristics a successful malicious attacker's software would have and what the assessment team's tools need to be able to replicate. During these defensive engagements, members of the assessment team frequently need to create custom scripts (i.e., software programs) to effectively assess the extent of the vulnerabilities by creating exploits, and to determine if a successful attack has taken place or is in progress.

Third, other commenters state that the proposed rule's controls on technology for the development of “intrusion software” could cripple legitimate cybersecurity research. To address cyber threats, technical information must be shared with experts across the globe. In order to identify and quickly counter threats, the cybersecurity industry relies heavily on collaboration with other companies within and outside of the United States, as well as independent experts around the world. Many of these experts are self-taught, have no prior formal relationship with cybersecurity firms, and, in many cases, may be unknown until they discover a new vulnerability. To address a vulnerability, a company must be able to engage in a back-and-forth dialogue with these researchers and experts. Often, the dialogue must include detailed discussion of exactly how a particular vulnerability could be exploited to gain control of a computer; without such discussion it is not possible to evaluate the risk posed by a vulnerability or to fashion an effective and comprehensive defense. Some commenters were concerned that, by subjecting vulnerability research, assessments, and testing to export licensing requirements including classification, screening, and other control elements, the control would limit the ability to fix and patch such vulnerabilities, leading to an overall decrease in the quality of cybersecurity. When vulnerabilities are discovered, they must be reported as soon as possible so that a fix can be developed. This process involves sharing not only the vulnerability and exploit, but also the technical information on how the exploits work, including the technology to develop them.

The commenters had many suggestions regarding how to address their concerns. The Administration will be reviewing all of them and many other ideas for how to address the policy objectives of the control but without unintended collateral harms. As I have said many times in response to questions about the rule, the only thing that is certain about the next step is that we will not be implementing as final the rule that was proposed. In working through this process, we will continue to seek input from those with expertise and equities in cyber security in both the U.S. government and the private sector before deciding in conjunction with its interagency partners what the next step should be. I thus welcome the Subcommittees’ inputs and am prepared to answer any questions you may have.