

Linda Dempsey

Vice President

International Economic Affairs

July 20, 2015

Regulatory Policy Division
Bureau of Industry and Security
U.S. Department of Commerce
Room 2099B
14th Street and Pennsylvania Ave. NW.
Washington, DC 20230.

Re: Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items (RIN 0694-AG49)

Via e-mail: PublicComments@bis.doc.gov

The National Association of Manufacturers (NAM) welcomes the opportunity to comment on the proposed rule issued by the U.S. Department of Commerce to implement the agreements by the Wassenaar Arrangement (WA) reached at the Plenary meeting in December 2013 regarding cybersecurity items like intrusion software and network surveillance systems.

The NAM is the nation's largest industrial trade association, representing small and large manufacturers in every industrial sector and in all 50 states. Today's connected environment allows manufacturers of all sizes to increase their productivity, speed innovation and take their businesses global. Manufacturers are entrusted with vast amounts of data through their comprehensive and connected relationships with customers, vendors, suppliers and governments. They are responsible for securing the data, the networks on which the data run and the facilities and machinery they control at the highest priority level. Additionally, manufacturers are the owners, operators and builders of our nation's critical infrastructure. They manufacture and use the temperature controls regulating the grain silos that store our food supplies. They build and manage the systems operating the traffic signals that set the rules of the road. They build and run the energy plants that power our homes and businesses as well as the heavy machinery exploring oil and gas fields. Manufacturers make technology products ranging from nanoscale electronic devices to fighter jets. Manufacturers leverage technology to design, produce and deliver these products, and technology is also used to manage, monitor and secure key facilities and products, including trade secrets and patents.

The products, controls, systems, patents, trade secrets and all other tools that differentiate manufacturers in the United States from their competitors abroad are vital to continued innovation and global competitiveness. The technology that enables and helps drive this innovation in the online environment has also created a new vulnerability: exposure to cyber thieves that are constantly attempting to penetrate networks to steal valuable intellectual property. This illegal activity allows bad actors to replicate products and designs and disrupt business activity and critical infrastructure. Manufacturers know they need to secure their networks, their controls and their data. Companies are engaged in ongoing efforts to strengthen their information technology networks and protect their IP, investing in information technology assets and hiring cybersecurity experts. Highly skilled cybersecurity researchers perform research, attend hacker conferences, network with their peers and then provide manufacturers and program managers with the tools to counter vulnerabilities. So-called "zero day" exploits are developed to demonstrate a suspected vulnerability, and the results from these exploits are then used to target and perform testing that ensures the vulnerability is resolved.

Leading Innovation. Creating Opportunity. Pursuing Progress.

The Department's proposed rule would require a license for the export, reexport, or transfer (in-country) of certain cybersecurity items to all destinations, except Canada. The proposed rule also contains Encryption Items (EI) registration and review requirements, while setting forth proposed license review policies and special submission requirements to address the new cybersecurity controls, including submission of a letter of explanation with regard to the technical capabilities of the cybersecurity items. The proposal also puts forth a new definition of "intrusion software" for the Export Administration Regulations (EAR), pursuant to the WA 2013 agreements.

The proposal touches on complex technical and policy issues, and the NAM urges the Commerce Department to take the necessary time to reconsider fully the proper approach to these controls. As an example, the Bureau of Industry & Security (BIS) could convene technical workshops for input and insight from industry and the security community. After gathering facts and insight through those discussions, we urge BIS to issue a new proposed rule that focuses on a narrower set of items and avoids imposing undue compliance burdens on legitimate cybersecurity efforts.

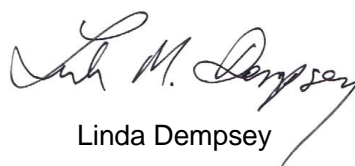
If implemented as currently drafted, the proposed rule would seriously impair the ability of manufacturers to identify and fix software and other security vulnerabilities, while requiring thousands of export licenses. As drafted, the proposed rule would require licenses for virtually all exports, reexports, and deemed exports of an overly broad set of controlled items. The projected number of activities and tools subject to licensing controls in the software and IT industries generally is expected to be staggering. The significant compliance burden would likely have an overall effect of actually diminishing security for individuals and enterprises because the sheer volume of activities covered under the proposed rule would impose unreasonable burdens on the processing capabilities of both manufacturers and BIS, rather than placing the resources and efforts on the areas that would best address concerns that BIS may have.

Moreover, the proposed rule would likely hamper the efforts of cybersecurity professionals to protect critical networks and infrastructure against malicious intrusion by imposing delays and restrictions on the use of the best available tools to maintain security.

Manufacturers create products that are used in the world's critical infrastructures, and it is vital that we continue to ensure that our products are as secure as possible. Part of a product's secure development lifecycle program is to perform various security assessments in order to discover vulnerabilities – whether those are product features that could be exploited or simply bugs in the programming that would enable an attacker to remotely control or configure a device. The proposed rule would unfortunately discourage companies from performing those security assessments efficiently and effectively.

Thank you for the opportunity to provide comments on the proposed rule to implement the WA 2013 agreements regarding cybersecurity items. Manufacturers remain committed to working with the Department of Commerce and other U.S. agencies to improve and streamline U.S. export control requirements that will promote U.S. economic, national security and foreign policy interests.

Thank you,

A handwritten signature in black ink, appearing to read "Linda M. Dempsey". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Linda Dempsey