

Testimony of

Dr. Phyllis Schneck
Deputy Under Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
United States Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
And the
Committee on Homeland Security

January 12, 2016

Introduction

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, and Ranking Member Richmond and distinguished members of the Committees, let me begin by thanking you for the unwavering support provided to the Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD). We look forward to continuing to work with you in the coming year to ensure a homeland that is safe, secure, and resilient against terrorism, cyber-attacks, natural disasters, and other risks.

In particular, we appreciate Congress' efforts in passing the Cybersecurity Act of 2015 last month. This invaluable legislation will significantly enhance our ability to exchange cybersecurity threat information between the government and the private sector and will improve our ability to protect federal civilian networks.

NPPD undertakes its cybersecurity activities within its overarching mission to secure and enhance the resilience of the Nation's cyber and physical infrastructure. We view ourselves as a customer service organization, and our customers are federal civilian departments and agencies, state, local, tribal, and territorial governments, and the private sector. NPPD strives to

understand the mission, interests and equities of all of our customers to build trusted relationships for knowledge exchange and to better enable their resilience by creating and offering the right services and capabilities.

Within the private sector, NPPD maintains a particularly close partnership with the cybersecurity community – developers, vendors, and researchers that create the innovative solutions to help protect our Nation from cybersecurity risk. It is in this context that we consider the 2013 Wassenaar Agreement on Intrusion and Surveillance Items. I appreciate the concerns raised by many Members of Congress.

By way of background, the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multi-lateral forum intended to promote transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies. In 2013, Participating States to the WA agreed upon a new export control for “systems,” “equipment,” or “components” thereof, “specially designed” or modified for the generation, operation or delivery of, or communication with, “Intrusion Software.” Pursuant to this unanimous agreement, the Department of Commerce engaged in a rulemaking process as the U.S. Government’s lead for domestic implementation of WA rules. Industry feedback to a Notice of Proposed Rulemaking (NPRM) was overwhelmingly negative and raised significant concerns regarding implications for cybersecurity innovation, research, and information sharing.

NPPD and the DHS Science and Technology Directorate, the Department’s export control lead, have further consulted with numerous industry groups and solicited feedback through the Sector Coordinating Councils. For context, Sector Coordinating Councils are structures of the National Infrastructure Protection Plan Framework that bring together executives in the private sector to collaborate with each other and with the U.S. Government on key issues of cyber and infrastructure protection, transcending the competitive boundaries that traditionally block this type of collaboration within a sector. Most of our critical infrastructure sectors have a Sector Coordinating Council. It is important to note that the private sector participants expend great energy, resources and intellectual capital in these Sector Coordinating Councils, because they

know that the government strongly considers the resulting sector views in future planning and policymaking.

DHS understands that there are national security concerns that led to the development of this control with the aim to restrict exports of such tools related to intrusion software so they cannot be used maliciously. However, we need to ensure that in implementing the 2013 control, the U.S. does not inadvertently create greater problems and more risks than the security concerns that the control was intended to address. The interagency, including DHS, shall consider carefully the concerns raised by U.S. industry and legitimate potential impacts on the Nation's cybersecurity.

As the Committee knows, cybersecurity is defined by rapid change. Technology is evolving at a faster pace than ever before. Our adversaries are also changing rapidly, and are constantly developing new tools and attacks to compromise critical networks, steal data, and potentially damage our physical infrastructure. In this environment, it is essential for cybersecurity researchers and developers to share information rapidly across borders in the interest of creating the next security solution or combating an emerging risk.

For example, national cybersecurity response teams (such as Computer Security Incident Response Teams (CSIRTs)) rely on timely and actionable information about cybersecurity threats and vulnerabilities from researchers and other independent experts. In the United States, our CSIRT resides within NPPD, and is called the United States Computer Emergency Readiness Team (US-CERT). US-CERT relies upon international counterparts on a daily basis to help identify, respond to, and mitigate cybersecurity risks that threaten government and critical infrastructure networks. A substantial portion of information sharing with cybersecurity researchers occurs across national borders and this needs to be taken into account in implementing export controls.

Finally, there is a critical need for increased and sustained investment in cybersecurity research and development, rather than less. In crafting our approach to implementing the Wassenaar control, we need to take this into account, as well as the uncertainty expressed by many cybersecurity firms regarding the specific types of information that can be shared with their foreign-based subsidiaries, or with their own foreign national employees within the United States, without a license.

Evolving and sophisticated cyber threats pose a considerable challenge to securing critical infrastructure and government systems. As such, governments should implement policies to incentivize innovative research in measurably effective cybersecurity.

The United States is fortunate to have many global leaders in cybersecurity research and innovation within our borders. We also need to ensure that implementation of the Wassenaar control does not unduly disadvantage these companies in a global competition with their international peers.

Of course, NPPD is fully conscious of the significant risks posed by certain surveillance tools and intrusion software. There are myriad examples of governments using such tools to spy on dissidents, constrain freedom of expression, and engage in extrajudicial monitoring. But such examples also exemplify why we must support improved cybersecurity. We need a balanced approach that both protects cybersecurity research and innovation and make it harder for authoritarian governments to monitor dissidents or for cyber criminals to steal data about U.S. citizens. The inherent nature of many “cyber technologies” is that they are technologically agnostic; that is, the same software that is used to test a company’s cybersecurity can be used to conduct unauthorized or illegal surveillance. This demonstrates the complexity of the issue, and why further discussion is needed.

The Wassenaar Agreement on Intrusion and Surveillance Items was developed in response to a legitimate concern: reducing the proliferation of dual-use technologies that are used for malicious surveillance or hacking. But in implementing that control we need to avoid unintended consequences on cybersecurity. In a threat environment where our adversaries continue to gain in sophistication, we cannot afford to unduly constrain development of the next generation of cybersecurity solutions. Cybersecurity developers and vendors must be able to share information for legitimate purposes as quickly as possible. Researchers must be able to share appropriately vulnerability and threat information with US-CERT and national CSIRTs in friendly states. The interagency continues to consider the issue. In the meantime, DHS will continue to support national security efforts undertaken at the Wassenaar Arrangement while continuing to work with our interagency partners to strengthen U.S. cybersecurity.