Statement for the Record

Of

Richard Driggers
Deputy Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the United States House of Representatives
Committee on Small Business

Regarding

Foreign Cybersecurity Threats to America's Small Businesses

January 30, 2018

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to be here today. Safeguarding and securing cyberspace is a core mission at the Department of Homeland Security (DHS). I am pleased to be here today discussing our efforts to reduce and mitigate cybersecurity risk to the Nation's small businesses.

The National Protection and Programs Directorate (NPPD) is responsible for protecting civilian Federal Government networks; sharing information related to cybersecurity risks and incidents and providing technical assistance to federal agencies, as well as state, local, tribal, and territorial (SLTT) governments, international partners and the private sector; and coordinating certain aspects of the Federal Government's incident response activities to defend against cyber threats. We endeavor to enhance cyber threat information-sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their networks and quickly recover should such a cyber incident occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing on best practices and cyber threats, and to strengthen resilience.

There are over 30 million small businesses in the U.S. employing over 47 percent of the Nation's population and comprising over 97 percent of total businesses in North America. As small businesses become increasingly reliant on information technology, so do the cybersecurity risks they face. Malicious cyber activity can severely harm small business operations and reduce consumer confidence. The Department of Homeland Security, Department of Justice, Small Business Administration, and other interagency partners play a crucial role in helping small businesses identify and mitigate these risks.

Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past year has marked a turning point in the cyber domain. We have long been confronted with a myriad of malicious cyber activities against our digital networks. But over the past year, Americans saw advanced persistent threat actors, including hackers, cyber criminals, and nation states, increase the frequency and sophistication of malicious cyber activity. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy through attempts to manipulate elections.

Global cyber incidents, such as the "WannaCry" ransomware incident in May of last year and the "NotPetya" malware incident in June, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. Incidents like these are indiscriminate, and the Nation's small businesses are often victims. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, NPPD had already taken actions to help protect networks from similar malicious cyber activities.

Through requested vulnerability scanning, NPPD helped stakeholders identify vulnerabilities on their networks so they could be patched before these cyber incidents occurred. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders. As the incidents unfolded, NPPD led the Federal Government's incident response efforts, working with our interagency partners, including providing situational awareness, information sharing, malware analysis, and technical assistance to affected entities.

Supporting the Nation's Small Businesses against Cyber Risks

Small businesses play a key role in ensuring the security, reliability, and resilience of the Nation's critical infrastructure. The Homeland Security Act authorizes NPPD's National Cybersecurity and Communications Integration Center (NCCIC) to assist small businesses through the dissemination of information on cyber threat indicators, defensive measures, cybersecurity risks, incidents, analyses, and warnings. Critical infrastructure owners and operators depend on small businesses to provide equipment and services and small businesses rely on having a reputation of a trusted business partner. It is essential that small businesses adopt common cybersecurity standards and practices to protect themselves and their customers. Small businesses face the same threats as large business, but do not necessarily have access to the same resources or information as large businesses. NPPD is working with our interagency partners to close the gap for cybersecurity information sharing, training, and resources.

The Federal Government and its contractors, subcontractors, and suppliers at all tiers of the supply chain are under constant attack, targeted by increasingly sophisticated and well-funded adversaries seeking to steal, compromise, alter or destroy sensitive information. In some cases, advanced threat actors target small businesses deep in the government's supply chain to gain a foothold and then pivot to sensitive information and intellectual property. Over the last several years, many federal contractors have significantly improved their cybersecurity posture, making it more difficult for threat actors to launch successful attacks on their enterprises. However, this has caused increased targeting of small businesses connected to the federal supply chain that may not have the resources or awareness to adequately address such threats.

DHS and the U.S. Small Business Administration have partnered to develop a strategy pursuant to the requirements in section 1841 of the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. No. 114-328) to help small and medium-sized businesses enhance their cybersecurity planning and risk management efforts.

In order to develop a strategy that effectively responds to stakeholders' needs, the America's Small Business Development Centers (ASBDC) conducted a nationwide survey soliciting feedback on the cybersecurity needs of small businesses. Over 85 percent of small business owners fear cyber incidents and feel unprepared to handle one. Despite the expressed need for resources to address cyber concerns, 70 percent of respondents said they were not aware of available resources and only 7.7 percent indicated they looked for resources from Federal Government sources. More than half of respondents indicated they need skills in small business defensive and response strategies.

These responses demonstrate the need to take a different approach engaging small businesses compared to large corporations or other federal agencies. Small businesses are diverse in size and complexity, with varying needs for improving their cybersecurity posture. For some, it may be basic training related to cyber hygiene and for others, it may be complex vulnerability assessments. To effectively address the cybersecurity needs of small businesses, the Federal Government must be able to identify the most relevant resources and information and provide those resources and information in an efficient and cost-effective fashion. This involves not only a centralized location with access to all existing federal cybersecurity information and resources, but also a way to match the appropriate resources to the specific needs of small businesses.

Fortunately, the Department of Homeland Security already offers or supports an array of cybersecurity programs, projects, and activities that are applicable to small businesses. In developing the small business development center cyber strategy, we identified at least 46 federal programs or initiatives that small businesses can utilize. Some programs were created specifically for small businesses, while others serve a larger critical infrastructure audience. Increasing awareness and access to these resources, which are available at little to no cost, can increase the cybersecurity of small businesses.

Furthermore, NPPD promotes cybersecurity tools, best practices, and services to the small business community. This is a focal point for cybersecurity outreach, education, and information for the Nation's 16 critical infrastructure sectors as well as small and medium-sized businesses. NPPD cybersecurity resources include technical assistance; voluntary assessments; sector-specific implementation guidance; cybersecurity publications for business and government agencies; cybersecurity awareness raising materials; a suite of services for conducting risk assessments and enhancing information sharing; and cyber workforce development and training programs. NPPD continues to work on expanding awareness of these resources among small businesses.

Information sharing and safeguarding information is a key pillar of effective cybersecurity. By appropriately sharing information while protecting personally identifiable information rapidly between government and the private sector, network defenders can block cyber threats or limit the effects of compromised systems. Last year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This EO set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. DHS has led collaborative efforts with federal and private sector partners to accomplish the range of actions included in the EO. Many of the initiatives NPPD has developed and improved upon can be applied to small businesses.

The NPPD's NCCCI serves as the hub of information sharing activities for DHS to increase awareness of vulnerabilities, incidents, and mitigation. Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is NPPD's flagship program for public-private information sharing and complements other DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. CISCP is free of charge and available to any company with an interest in multi-directional cybersecurity information sharing and robust collaboration.

By sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures.

Moreover, as required by the Cybersecurity Act of 2015, we established a capability, known as Automated Indicator Sharing (AIS), to automate our sharing of cyber threat indicators in real time. AIS is a part of the Department's effort to create an environment where as soon as a company or federal agency observes an attempted compromise, the indicator is shared at machine speed with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of malicious cyber activities, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense-in-depth should enable organizations to detect and thwart the most common malicious cyber activity, freeing their cybersecurity staff to concentrate on the novel and sophisticated malicious cyber activity.

More than 230 agencies and private sector partners have connected to the AIS capability. Notably, partner organizations include partners, information sharing and analysis organizations (ISAOs) and computer emergency response teams, which further share with or protect their customers and stakeholders, significantly expanding the impact of this capability and accessibility to smaller businesses. The AIS technologies and policy are structured in a way that protects the identity of our partners, and the information shared is limited to cyber threat information, which protects privacy and civil liberties. AIS is still a new capability and we expect the volume of threat indicators shared through this system to substantially increase as the technical standards, software, and hardware supporting the system continue to be refined and put into full production. As more indictors are shared from other federal agencies, SLTT governments, and the private sector, this information sharing environment will become more robust and effective. This approach to collective defense helps ensure that small and medium-sized businesses are protected using the best defense information available, including information from larger and more sophisticated companies and our own government sources.

Supply Chain Risk Management

Supply chain risk is another area that has gained increasing prominence and concern in recent years. When the Federal Government—or its contractors at any tier of the supply chain—acquire a solution that has inadequate cybersecurity built in, the government ultimately incurs increased risk throughout the lifespan and disposal of that product or service. This remain the case until the government incurs the often more expensive cost of fixing the vulnerability after its incorporation. The lasting effect of inadequate built in cybersecurity in acquired items is part of what makes supply chain risk management so important to achieving cybersecurity and resiliency.

Offshore sourcing by information and communications technology (ICT) manufacturers and sellers has demonstrated its merit as a means to reduce costs. And as a result, most ICT is now produced in a global supply chain. Movement of production outside the U.S. has led to growing concerns associated with foreign ownership, control, manipulation, or influence over

items that are purchased by the government and used in or connected to critical infrastructure or mission essential systems.

To appropriately address supply chain risks, it is critical to understand that the problem is not a simple function of geography. While there are certainly countries that provide environments that are more conducive to nefarious supply chain activities, pedigree is only a sub-set of factors to consider in supply chain risk assessments. There are more important factors to address the security or integrity of components and end items, including careful attention to the people, processes, and technology used to develop, deliver, operate, and dispose of the products and services used by the government and its contractors. Additionally, it is important to note that most known incidents are not caused by an adversary intentionally inserting malicious code into an ICT component through its supply chain, but are made through exploitation of unintentional vulnerabilities in code or components due to inadequate security practices in the manufacturing and integration processes.

Last year, the President signed EO 13806 on *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States.* The Department of Homeland Security has worked with the Department of Defense to identify key supply chain risks. In parallel to this, NPPD has established a Cyber Supply Chain Risk Management (C-SCRM) Initiative under the Office of Cybersecurity and Communications to address risks to our ICT supply chains. The objective of the C-SCRM initiative is to enable stakeholders to be smarter consumers of ICT products and services by providing timely, robust, actionable information about supply chain risks and mitigations to users, buyers, manufacturers, and sellers of ICT.

While the ICT supply chain is not the source of all cyber risk, it presents opportunity for creation of threats and vulnerabilities, and ICT enables the connectivity that is a necessary element for cyber exploitation. Commercial ICT is ubiquitous in federal networks, even those that handle the most sensitive information and support essential functions of the government. Therefore, the C-SCRM Initiative will focus primarily on exposure to cyber risks related to acquisitions of ICT and how those risks should be addressed. However, due to the increasing connectivity of the world and the growing sophistication of threats, the initiative will also address acquisitions that are outside the boundaries of traditional definitions of ICT, including connected Internet of Things devices such as automobiles and industrial control systems. In 2018, the C-SCRM initiative will begin identifying and mitigating supply chain threats and vulnerabilities to Federal High Value Assets. In the following year, the C-SCRM Initiative will expand in scope to conduct due diligence on proposed contractors and subcontractors for individual acquisitions, provide public-private stakeholders unclassified supply chain risk information, and establish trusted supplier and product lists.

Conclusion

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the Federal Government's efforts to defend our Nation's critical infrastructure from natural disasters, terrorism and adversarial threats, and technological risk such as those caused by cyber threats. Our infrastructure environment today is complex and dynamic with interdependencies

that add to the challenge of securing and making it more resilient. Small businesses play an important role in protecting and securing our Nation's critical infrastructure as they are important players in effective supply risk management. The Federal Government possesses a suite of programs and capabilities that can improve cybersecurity for small businesses. However, not all small businesses require the same type of resources. DHS is able offer a range of services to meet these needs and continues to pursue new opportunities to provide assistance. As our Nation continues to evolve and new threats emerge, we must not only develop more effective methods to safeguard our information systems, but also find more cost-effective and efficient ways to increase public awareness and access to cybersecurity resources.

Thank you for the opportunity to testify, and I look forward to any questions you may have.