STATEMENT OF

U.S. DEPARTMENT OF HOMELAND SECURITY

SORAYA CORREA

CHIEF PROCUREMENT OFFICER, OFFICE OF THE CHIEF PROCUREMENT OFFICER

U.S. DEPARTMENT OF HOMELAND SECURITY

DR. JOHN ZANGARDI

CHIEF INFORMATION OFFICER, OFFICE OF THE CHIEF INFORMATION OFFICER

U.S. DEPARTMENT OF HOMELAND SECURITY

JEANETTE MANFRA

ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

U.S. DEPARTMENT OF HOMELAND SECURITY

FOR A JOINT HEARING TITLED

"ACCESS DENIED: KEEPING ADVERSARIES AWAY FROM THE HOMELAND SECURITY SUPPLY CHAIN"

BEFORE THE

SUBCOMMITTEES ON COUNTERTERRORISM AND INTELLIGENCE

AND

OVERSIGHT AND MANAGEMENT EFFICIENCY

OF THE

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY

JULY 12, 2018

Introduction

Chairman King, Chairman Perry, Ranking Member Correa, Ranking Member Rice, and members of the Subcommittees, thank you for this opportunity to discuss with you ways to improve the Department of Homeland Security's (DHS) ability to effectively manage supply chain risk. The Secretary of DHS has two primary sets of supply chain risk management responsibilities related to information and communications technology (ICT). In one set, the Secretary is responsible for procurement and supply chain risk management within DHS's ICT environment. These responsibilities are carried out by the DHS Chief Procurement Officer (CPO) and DHS Chief Information Officer (CIO). In carrying out the other set of responsibilities, the Secretary of DHS, in consultation with the Office of Management and Budget (OMB), administers the implementation of government-wide information security policies and practices. These responsibilities are carried out by the National Protection and Programs Directorate (NPPD).

ICT is critical to an agency's ability to carry out its mission efficiently and effectively. Supply chain risks could contribute to the loss of confidentiality, integrity, or availability of information or information systems and result in adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Cyber Supply Chain Risk Management (C-SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. C-SCRM spans the entire life cycle of ICT, including design, development, acquisition, distribution, deployment, maintenance, and product retirement.

Current Supply Chain Risks

The ICT supply chain is widely viewed as a source of significant risk to ICT products, systems, and services. Vulnerabilities in ICT can be exploited intentionally or unintentionally through a variety of means, including deliberate mislabeling and counterfeits, unauthorized production, tampering, theft, and insertion of malicious software or hardware. If these risks are not detected and mitigated, the impact to the ICT could be a fundamental degradation of its confidentiality, integrity, or availability and potentially adverse impacts to essential government or critical infrastructure systems.

Increasingly sophisticated adversaries seek to steal, compromise, alter, or destroy sensitive information on systems and networks, and risks associated with ICT may be used to facilitate these activities. The Office of the Director of National Intelligence (ODNI) acknowledges, "The U.S. is under systemic assault by foreign intelligence entities who target the equipment, systems, and information used every day by government, business, and individual citizens."[1] The globalization of our supply chain can result in component parts, services, and manufacturing from sources distributed around the world. ODNI further states, "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property and personally identifiable information, insert malware into critical

[1] https://www.dni.gov/files/NCSC/documents/products/20170317-NCSC--SCRM-Background.pdf

components, and mask foreign ownership, control, and/or influence (FOCI) of key providers of components and services."

Managing Information as a Strategic Resource

Current law governing information security of federal information resources requires agencies to implement an agency-wide information security program that ensures that information security is addressed throughout the life cycle of each agency information system (44 U.S.C. 3554(b)). On July 27, 2016, OMB released an update to Circular A-130, *Managing Information as a Strategic Resource*, the federal government's governing document for management of Federal information resources. Among other things, the revisions require agencies to establish a comprehensive approach to improve the acquisition and management of their information resources. This includes requirements for agencies to implement and oversee the implementation of supply chain risk management principles to protect against the insertion of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software throughout the system development life cycle. Moreover, appropriate supply chain risk management plans to ensure the integrity, security, resilience, and quality of information systems are described in the National Institute of Standards and Technology (NIST) Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

The Current Rules for Unclassified Procurements

C-SCRM is no longer an emerging threat, it is pervasive. However, the rules under which procurements are conducted have not kept pace with the evolution of this threat. The Federal Acquisition Regulation is designed to balance the equities of the contracting parties, ensuring due process for contractors and full disclosure of the government's reasons for pursuing contractual remedies in the event of performance or integrity failure. These rules, however, were designed around the procurement of commodities and services that were not anticipated to be vulnerable to, nor the target of, the sophisticated foreign intelligence activities witnessed in recent years, especially those associated with a globalized ICT supply chain. For instance, the current procurement rules and their underpinning statutes did not imagine the need to use and protect intelligence information in unclassified procurements. While there are tools available to pursue correction of contractor performance issues or address integrity failures, they do not provide the flexibility to react swiftly to or protect intelligence information when exclusion of a source is the only way to mitigate supply chain risk. In fact, some currently available procurement tools that address performance issues, such as government-wide exclusion from doing business with any agency for a period of time, are too harsh, unless an agency investigation deems the contractor to be at fault for the performance issue. New rules are needed to combat the threat to our Nation's federal information technology networks when intelligence information identifies risks that cannot be mitigated.

Using and Protecting Intelligence Information

Gaps exist in the DHS's authority to use intelligence information to support its procurement decisions when a significant supply chain risk cannot be mitigated. Mitigation, which is an action initiated by the government to preclude a supply chain risk from causing a security concern, is the preferred and least disruptive method of addressing supply chain risk. However, in those exceptional cases where mitigation is not possible, DHS does not have the capability to react swiftly while appropriately restricting disclosure of intelligence and other national security sensitive information.

DHS Cyber Supply Chain Risk Management (C-SCRM)

In order to appropriately manage supply chain risks, stakeholders need increased visibility into, and understanding of, how the products and services they buy are developed, integrated, and deployed, as well as the processes, procedures, and practices used by ICT manufacturers and purveyors to assure the integrity, security, resilience, and quality of those products and services. The DHS Office of the Chief Information Officer (OCIO) has initiated work focused on establishing a C-SCRM effort executed department-wide.

The effort will include a governance structure that will update existing policy and procedures for C-SCRM. Documentation will be developed that will align with current policies while providing programmatic subject-matter expertise to DHS stakeholders and risk owners. Integral to the success of these efforts will be the functions and capabilities to conduct vulnerability and threat identification and analysis. To accomplish this, a process will be established to produce timely supply chain risk assessments of companies, products, and services based on an analysis of publicly and commercially available information about the company and product, or service being purchased and information shared through liaisons with the U.S. Intelligence Community (IC) threat assessment centers and DHS Office of Intelligence and Analysis (I&A), as appropriate.

Working closely with NPPD and the DHS CPO, the initiative will develop education and training to ensure the effective use of the new authority. Guidance will also be provided to assist buyers in determining criticality, priority, and risk tolerance for the product or service to be purchased as well as assisting buyers and sellers with determining mitigation actions where supply chain risks have been identified.

The DHS CIO knows first-hand that all tiers of the supply chain are targeted by increasingly sophisticated and well-funded adversaries seeking to steal, compromise, alter, or destroy information and is committed to establishing a robust enterprise approach to better managing the risk and vulnerabilities associated with ICT components. Although DHS is investing in C-SCRM with the goal to broaden and further strengthen our approach, additional authority is needed to ensure that risk is assessed and mitigated in a timely manner, and that disclosure of intelligence sources and other information is restricted.

Government-Wide Cyber Supply Chain Risk Management (C-SCRM)

The Administration has been working to establish a strategic statutory framework to protect our Federal supply chain by conducting supply chain risk assessments, creating mechanisms for sharing supply chain information, and establishing exclusion authorities—both within agencies and in a centralized manner—to be utilized when justified. Earlier this week, the Administration shared its proposed legislation with Congress, the "Federal Information Technology Supply Chain Risk Management Improvement Act of 2018." We look forward to supporting the Administration's work with Congress on the bill and strengthening our ability to help agencies execute departmental missions in an environment of changing vulnerabilities and threats.

NPPD carries out the DHS Secretary's responsibilities to administer the implementation of government-wide information security policies and practices (44 U.S.C 3553(b)). These statutory responsibilities include monitoring agency implementation; convening senior agency officials; coordinating government-wide efforts; providing operational and technical assistance; providing, as appropriate, intelligence and other information about cyber threats, vulnerabilities, and incidents to agencies; and developing and overseeing implementation of binding operational directives, among other actions. DHS leverages the full range of authorities to address supply chain risks across the federal government.

DHS is working with the Department of Defense (DOD), the intelligence community, and other agencies to address key supply chain risks. In January 2018, NPPD established a C-SCRM initiative to centralize DHS's efforts to address risks to the ICT supply chains of federal agencies, critical infrastructure owners and operators, and state, local, tribal, and territorial governments. The mission of the C-SCRM initiative is to identify, assess, prevent, and mitigate risks associated with ICT product and service supply chains throughout the lifecycle. Initially this initiative will focus on identifying and addressing supply chain risks related to the federal government's high-value assets (HVAs), or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to U.S. national security interests, foreign relations, the economy, or to the public confidence, civil liberties, or public health and safety of the American people. Additionally, DHS, in partnership with the General Services Administration, is working to bridge the gap between the procurement and ICT professional by providing acquisition professionals with awareness, training, and educational content to be available through the Federal Acquisition Institute.

Since 2017, NPPD now requires Continuous Diagnostics and Mitigation (CDM) vendors to complete a SCRM questionnaire as part of their application to place a product on the CDM approved products list. The questionnaire provides information to agencies about how the vendor identifies, assesses, and mitigates supply chain risks in order to facilitate better informed decision-making. The information is intended to provide visibility into, and improve the buyer's understanding of, how the products are developed, integrated, and deployed; as well as the processes, procedures, and practices used to assure the integrity, security, resilience and quality of those products.

Intelligence Support and Countering Illicit Activity

Despite the gaps in DHS's ability to use intelligence information to support its procurement actions, DHS has a variety of efforts currently underway within our existing authorities to help address these risks. One such effort is the strengthening of our counterintelligence capabilities. These capabilities include resources within DHS I&A as well as strengthening partnerships across other key components of the U.S. IC. Additionally, DHS Components, including the U.S. Secret Service, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement, play a critical role in identifying and disrupting illicit activity impacting supply chain risk. In collaboration with the Federal Bureau of Investigation, and the Departments of State, Treasury, Commerce, and Defense, we are actively leveraging our individual and collective authorities to counter malicious actors and mitigate supply chain risks.

Conclusion

As DHS looks at the current threat landscape and the risk posed by increasingly sophisticated adversaries, we appreciate the Committee’s interest in supply chain risk management and look forward to working with the Members and your staff on these issues. Thank you for the opportunity to testify before the Subcommittees. We are happy to answer any questions you may have.