Written Testimony

of

Jeanette Manfra

Acting Deputy Under Secretary for Cybersecurity

National Protection and Programs Directorate

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Subcommittee on Cyber and Infrastructure Protection

Committee on Homeland Security

Regarding

Federal Network Cybersecurity

March 28, 2017

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and members of the Committee, thank you for the opportunity to appear before you today. Cybersecurity remains one of the most significant strategic risks to the United States. The past several years have seen a steady drumbeat of cybersecurity compromises affecting the Federal Government, state and local governments, and the private sector. Working with Congress, we have focused on a range of actions to confront this evolving challenge. 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 sharing of information on best practices and cyber threats, and strengthen resilience. The Department of Homeland Security (DHS), through the National Protection and Programs Directorate (NPPD), leads the federal government's efforts to secure our Nation's critical infrastructure and protect federal civilian networks from malicious cyber activity.

Over the past few years, the federal government has made significant progress in improving agency cybersecurity, establishing a common baseline of protection, and codifying roles and responsibilities to effectively manage cybersecurity risks and incidents. Through engagements with state, local, tribal, and territorial (SLLT) governments, and the private sector, we have provided technical assistance upon request and expanded information sharing capabilities to improve situational awareness of threats, vulnerabilities, incidents, mitigation, and recovery actions. Today, I will discuss the roles of NPPD in protecting the federal civilian executive branch networks.

Under the *Federal Information Security Modernization Act of 2014* (FISMA), agencies have primary responsibility for their own cybersecurity, the Office of Management and Budget

(OMB) generally develops and oversees agency implementation of information security policies and practices, and DHS administers the implementation of those policies and practices. As part of securing their own systems, agencies must comply with OMB policies, DHS directives, and National Institute of Standards and Technology (NIST) standards and guidelines. DHS, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps agencies manage their cyber risk. NPPD's assistance to agencies includes (1) providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes EINSTEIN, and Continuous Diagnostics and Mitigation (CDM) programs, (2) measuring and motivating agencies to implement policies, directives, standards, and guidelines, (3) serving as a hub for information sharing and incident reporting, and (4) providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services. DHS's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination.

EINSTEIN

EINSTEIN refers to the suite of intrusion detection and prevention capabilities that protects agencies' unclassified networks at the perimeter of each agency. EINSTEIN provides situational awareness of civilian executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

The first two phases of EINSTEIN – EINSTEIN 1 and 2 – allow DHS to identify potentially malicious activity and to conduct critical analysis after an incident occurs, as well as to detect known malicious traffic. In 2015, DHS estimated these capabilities screened over 90 percent of all federal civilian Internet traffic. On a typical day, EINSTEIN 2 intrusion detection sensors generate approximately 30,000 alerts about potential malicious cyber activity. These alerts are evaluated by DHS cybersecurity analysts to determine whether the alert represents an active threat and potential compromise, and if further mitigation or remediation is needed.

EINSTEIN 3 Accelerated (EINSTEIN 3A) is the intrusion prevention capability, which blocks known malicious traffic. Intrusion prevention is provided as a service by Internet service providers (ISPs) serving the federal government. The initial implementation of EINSTEIN 3A involves two intrusion prevention security services by the ISPs: domain name server (DNS) sinkholing and email filtering. DHS is working with the ISPs to add further protections. EINSTEIN 1 and 2 use only unclassified cyber threat indicators, while EINSTEIN 3A uses unclassified and classified indicators. These signature-based capabilities use indicators of compromise to detect and block known malicious traffic.

In the Cybersecurity Act of 2015, Congress directed each executive branch civilian agency to apply available EINSTEIN protections to all information traveling to or from an agency information system by December 18, 2016. Agencies have made significant progress in implementing available EINSTEIN protections. Prior to passage of the Act, EINSTEIN 3A covered approximately 38 percent of federal civilian users. Today, EINSTEIN 3A is protecting a significant percentage of the executive branch civilian workforce at the 23 largest agencies and most agencies have at least one of its two intrusion prevention capabilities. DHS continues to work with all remaining federal civilian agencies to facilitate their full participation in

EINSTEIN. At the same time, our NCPS program is also developing new capabilities and conducting a strategic review of the program architecture that will provide even more protections for federal agencies.

Today, EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity. Leveraging existing investments in the ISP infrastructure, our non-signature based pilot efforts to move beyond current reliance on signatures are yielding positive results in the discovery of previously unidentified malicious activity. DHS is demonstrating the ability to capture data that can be rapidly analyzed for anomalous activity using technologies from commercial, government, and open sources. The pilot efforts are also defining the future operational needs for tactics, techniques, and procedures as well as the skill sets and personnel required to operationalize the non-signature based approach to cybersecurity.

SLTT governments are able to access intrusion detection and analysis services through the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC's service, called Albert, closely resembles EINSTEIN 2. While the current version of Albert cannot actively block known cyber threats, it can alert cybersecurity officials to an issue for further investigation. DHS worked closely with MS-ISAC to develop the program and considers MS-ISAC to be the principal conduit for sharing cybersecurity information with state governments.

Continuous Diagnostics and Mitigation (CDM)

EINSTEIN, our tool to address perimeter security will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense in depth strategy that cannot be achieved through only one type of tool. CDM provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard. CDM is divided into four phases:

- CDM Phase 1 identifies all computers and software on agency networks and checks for known vulnerabilities.
- CDM Phase 2 allows agencies to better manage identities, accounts, and privileges for the people and services using their networks.
- CDM Phase 3 will assess activity happening on agencies' networks to identify anomalies and alert security personnel.
- CDM Phase 4 will protect sensitive and high value data within agency networks.

Significant progress has been made in the deployment of CDM. DHS has assessed the needs of the executive branch civilian agencies and has completed the purchasing of most CDM Phase 1 tools. Agencies are now installing the tools across their networks, including six agencies that have fully deployed all Phase 1 tools as well as the agency dashboards, which give network administrators visibility into the current state of their networks to better identify and prioritize areas of cyber risk. DHS has also awarded two CDM Phase 2 contracts, focusing on strong authentication for administrative users as well as general users, making the associated tools available to all participating agencies.

This summer, CDM will begin supplementing the existing CDM agency dashboards by introducing the federal CDM Dashboard, which will provide the National Cybersecurity and Communications Integration Center (NCCIC) with greater insight into the federal enterprise cybersecurity posture. The summary data available at the federal level presents a view of the relative risk and network health across the federal government to inform policy decisions and operational guidance, provide timely reporting for addressing critical issues affecting multiple agencies, and enable cost-effective and efficient FISMA reporting.

CDM will help us achieve two major advances for federal cybersecurity. First, agencies will have visibility, often for the first time, into the extent of cybersecurity risks across their entire network and gain the ability to prioritize identified issues based upon their relative importance. Second, the NCCIC will be able to identify systemic risks across the civilian executive branch. An example is illustrative. Currently, when a vendor announces a major vulnerability, the NCCIC tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will allow the NCCIC to immediately view the prevalence of a given device or software type across the federal government so that the NCCIC can provide agencies with timely guidance on their risk exposure. Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

CDM tools are currently available through blanket purchase agreement negotiated by the General Services Administration on DHS's behalf. This agreement leverages the government-wide volume to provide the best value and cost savings to the Federal Government. For example, by grouping agency requirements in Phases 1 and 2, we have saved the federal government millions of dollars on product purchases. Many SLTT governments are also able to purchase tools from this purchase agreement. By purchasing commercial CDM tools, SLTT governments can take advantage of bulk purchasing cost savings and invest those savings in their own cybersecurity resilience.

Measuring and Motivating Agencies to Improve Cybersecurity

DHS conducts a number of activities to measure agencies' cybersecurity practices and work with agencies to improve risk management practices.

The Cybersecurity Framework, is voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk and was developed by NIST through collaboration with diverse parts of industry, academia, and government, including DHS. TDHS promotes the use of NIST standards, guidelines, minimum information security requirements, including the Cybersecurity Framework.

FISMA provided the Secretary of Homeland Security with the authority to develop and oversee implementation of binding operational directives to agencies. In 2016, the Secretary issued a binding operational directive on securing high value assets (HVA), 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 the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. DHS works with several interagency partners to prioritize HVAs for assessment and remediation activities across the federal government. For instance, DHS conducts security architecture reviews on these HVAs to help agencies assess their network architecture and configurations.

As part of the effort to secure HVAs, DHS conducts in-depth vulnerability assessments of prioritized agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which DHS hackers send emails to agency personnel and test whether recipients click on potentially malicious links. DHS has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. These assessments provide system owners with recommendations to address identified vulnerabilities. DHS provides these same assessments, on a voluntary basis upon request, to private sector and SLTT partners. DHS also works with GSA to ensure our industry partners can provide assessments that align with our HVA initiative to agencies, if necessary.

Another binding operational directive issued by the Secretary directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing devices. The NCCIC conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's binding operational directive and have sustained this progress. When the Secretary issued this directive, NPPD identified over 360 "stale" critical vulnerabilities across federal civilian agencies. By "stale" I mean the vulnerabilities had been known for at least 30 days and were still not patched. Since December 2015, DHS has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly once they were identified.

By conducting vulnerability assessments and security architecture reviews, DHS is helping agencies find and fix vulnerabilities, and secure their networks before an incident occurs.

Information Sharing

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

Congress authorized the NCCIC as the civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. 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 protects the privacy and civil liberties of individuals by narrowly tailoring the information shared to that which is necessary to characterize identified cyber threats, consistent with longstanding DHS policy and the requirements of the Act. AIS is a part of the Department's effort to create an ecosystem in which as soon as a company or federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing limits the scalability of any attack techniques, which increases the costs for adversaries and should reduce the impact of malicious cyber activity. An ecosystem built around automated sharing and network defense should enable organizations to enhance their defenses against the most common cyber-attacks, freeing their cybersecurity staff to concentrate on the novel and sophisticated attacks. Over 129 agencies and private sector partners have connected to DHS's AIS capability. Notably, partners such as information sharing and analysis organizations (ISAOs) and computer emergency response teams further share with or protect their customers and stakeholders, significantly expanding the impact of this capability. 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.

Another part of the Department's overall information sharing effort is to provide federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis (I&A) is continuously assessing the specific threats to federal networks using traditional all source methods and indicators of malicious activity observed by NCCIC sensors so that the NCCIC can share with federal network defenders in collaboration with I&A. I&A personnel sit on the NCCIC watch floor.

Incident Response

Cybersecurity is about risk management, and we cannot eliminate all risk. Partners that implement best practices and share information will increase the cost for malicious actors and stop many threats. But ultimately, persistent adversaries will find ways to infiltrate networks in both government and the private sector. In Fiscal Year 2016, the NCCIC received reports of 30,899 impactful incidents across the eight attack vectors at federal agencies, according to the FISMA Annual Report to Congress. When an incident does occur, the NCCIC offers assistance upon request to find the adversary, drive them out, and restore service.

Conclusion

At all levels, the federal government continues to be targeted by a wide range of malicious cyber actors attempting to gain access to sensitive systems. We have made significant progress over the past year: we have provided a baseline of CDM Phase 1 tools, we have expanded the coverage of EINSTEIN 3A, we have expanded risk and vulnerability assessments, we have operationalized the automated indicator sharing capability, and we have established a useful architecture for coordinating the Federal Government's response to significant cyber incidents. But there is more to be done. This Administration will make significant investments in cybersecurity. In the recently-released budget blueprint, the President requested $1.5 billion for DHS to safeguard cyberspace by protecting federal networks and critical infrastructure from an attack. Through a suite of advanced cybersecurity tools and more assertive defense of government networks, NPPD would share more cybersecurity incident information with other Federal agencies and the private sector, leading to faster responses to cybersecurity attacks.

We must also ensure that DHS is appropriately organized to address today's and tomorrow's cybersecurity threats, and we appreciate the Chairman of the Committee's leadership in working to reauthorize the Department. As the committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that ensures a homeland that is more safe, secure, and resilient.

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

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu