COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

MAY 26, 2016

STATEMENT FOR THE RECORD

MARTI ECKERT
CHIEF INFORMATION SECURITY OFFICER
SOCIAL SECURITY ADMINISTRATION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me to discuss information security at the Social Security Administration (SSA), including our agency's compliance with the Federal Information Security Management Act (FISMA) and the Committee's scorecard on the Federal Information Technology Acquisition Reform Act. As the agency's Chief Information Security Officer, I support our Chief Information Officer in our agency's commitment to protect the information we manage and our systems from threats and vulnerabilities.

The security of the personally identifiable information (PII) the agency holds is of the utmost importance, and we take seriously our responsibility to protect the information provided to us by the public we serve. The agency has a strong, proactive approach to the identification and mitigation of risks associated with our online authentication to access public services via the internet, external and internal access to our secure network, and our information and communications assets. While we have strong controls in place, we know that there is no perfect way to lock down any system. In today's escalating threat environment, every cybersecurity program is a practice of continuous improvement.

Consequently, we continually work to keep pace with advancements in cybersecurity technology. We strengthen our security by remediating gaps in our security posture and institutionalizing and maturing security processes. We take a risk-based approach and leverage current agency processes, as we add layers of defense to improve protections and identify threats. Below, I will discuss in brief our cybersecurity program and some of the measures we are taking to counter potential cyber threats. Given the sensitive nature of this issue, I am unable to provide a detailed description of our cybersecurity capabilities in a public forum. However, I would be pleased to offer to you and your Committee staff a confidential briefing on this important issue.

Defense in Depth Strategy

At SSA, we employ a dynamic enterprise-wide cybersecurity program leveraging a defense-in-depth strategy to help protect our network, data, and employees while enabling the Agency's mission and meeting customer expectations in a safe and secure environment. We work diligently to protect our information, detect attacks, identify suspicious activities, and systematically respond to software and hardware vulnerabilities. We collaborate with the Department of Homeland Security's (DHS) United States Computer Emergency Response Team (US-CERT), the White House National Security staff, the Federal Chief Information Officer, and various law enforcement agencies to address cyber threats. We realize that technical solutions alone cannot combat adversarial threats in today's threat landscape, and it is not a single technology or process that keeps Social Security information safe, but rather an integrated, holistic approach comprised of many different technologies, processes, procedures, standards, guidelines and awareness programs. Our defense-in-depth strategy is composed of the following seven layers:

- A perimeter security layer, which deploys gateway protections where we connect to the external world;
- A network security layer, which houses the cybersecurity protections on our internal network;

- An endpoint security layer, which includes the security tools and technologies deployed on our laptops, workstations and mobile devices;
- An application security layer; which are the controls around our Social Security software applications;
- A data security layer, which are specific protections around our data;
- A prevention layer, which are those processes that allow us to identify gaps in our cybersecurity posture and address them; and
- A monitoring and response layer, which includes the protections in place to identify and respond to an incident.

Federal Cyber Sprint and the Cross-Agency Priority CyberSecurity Goals

I will now discuss the Agency's performance on the Federal Cyber Sprint and the Cross-Agency Priority CyberSecurity goals.

Cyber Sprint of 2015: We continue to build on the work we initiated last July as part of the federal Cyber Sprint. During the Cyber Sprint, agencies focused on multi-factor authentication, privileged users, remediating critical vulnerabilities identified by DHS, and assessing high value information assets. A brief status of our efforts is below.

Multi-Factor Authentication - Personal Identity Verification (PIV) cards
One way to enhance the protection of agency data is to ensure employees utilize their Personal Identity Verification (PIV) card when logging onto agency computer systems. This two-factor authentication method makes it harder for unauthorized individuals to gain access to SSA's network and systems and better protects sensitive agency data. We have issued PIV cards to 100% of the privileged users and 88% of unprivileged users on our network. We have a plan for completing the issuance of the remaining group of users in the State Disability Determination Services (DDSs) by December 2016.

Privileged Account Management
During the Cyber Sprint, we reduced the number of network privileged users in the Agency by 10 percent, and we continue to focus on controlling privileged accounts. Privileged accounts are user accounts with administrative privileges that possess a greater level of access than a regular user account. SSA is deploying new technology, which will allow us to control privileged accounts to a much greater degree, by letting users check out privileges only when needed, instead of having them assigned permanently. This will reduce the risk of these privileged accounts being compromised and used for malicious purposes.

Remediating Critical Vulnerabilities
The Agency was an early adopter of cyberhygiene scanning by the DHS. Weekly and on an ad-hoc basis, as needed, DHS scans SSA-owned IP ranges for vulnerabilities. SSA is one of ten Chief Financial Officer (CFO) Act Agencies that do not have any critical vulnerabilities as identified on DHS' Federal Cyber Exposure Scorecard.

Assessing High Value Assets

We assessed and prioritized the SSA systems and data sources that utilize PII. We conduct regular security assessments of our high value assets including vulnerability and penetration tests. We are currently undergoing our second exercise with DHS to assess the controls around our highest value assets. Such assessments are designed to emulate the attacks of real-world adversaries.

Cross-Agency Priority (CAP) CyberSecurity Goals: SSA meets all nine of the CAP CyberSecurity Goals. These goals focus on the implementation of the continuous monitoring of hardware assets, software assets, configurations and vulnerabilities, the implementation of multi-factor authentication, and malware and anti-phishing defenses.

Cybersecurity Best Practices at SSA

We are often asked to share some of our best cybersecurity practices with other federal agencies. The following section outlines some of those practices.

Incident Response and our Security Operations Center: We have a robust Incident Response Plan that details the roles and responsibilities of Agency personnel involved in a response to a cyber incident or breach. These roles include personnel from all facets of the agency, including our Security Operations Center (SOC). The agency has an internal Security Operation Center (SOC) staffed without interruption that monitors the agency's network environment to identify and detect suspicious activities, react to potential cybersecurity incidents, and ensure uninterrupted service delivery. The SOC leverages many technologies and capabilities to enable fast and accurate threat detection, remediation, and response to security incidents across the enterprise. Best practices in our SOC that we have shared with other federal agencies include:

- A centralized repository and automated workflow for reporting PII loss incidents within the Agency and for reporting all suspicious incidents to US-CERT.
- An automated solution that monitors when any user may be sending PII outside of the Agency in a non-secure manner. The program alerts and notifies management of any user that violates agency policy.
- Dashboards using a data aggregation tool that allow for trending incident data and reporting to agency executives. These metrics and reports improve executive decision-making by highlighting anomalies and providing data visualization.
- A strong working relationship with US-CERT while sharing information on all cyber-related incidents.
- Regular incident response exercises for both internal incidents (discovered by SSA) and external incidents (discovered by a third party). These tabletop exercises simulate the agency's response to an incident. Each scenario identifies roles and responsibilities of specific SSA parties or components for each particular situation and provides a low-stress opportunity to practice incident response.

Enterprise Penetration Testing Program: One of our most effective information security defenses is our Enterprise Penetration Testing program, which we implemented in 2012. It has become a cornerstone of our cybersecurity program to defend against hacks and data breaches. Penetration testing is the method of evaluating the security of a computer system or network by

simulating an attack from malicious outsiders who do not have authorized access to our systems and insiders who have some level of authorized access. The process involves analyzing the system for potential vulnerabilities that result from system misconfigurations and software flaws, both known and unknown. We have a dedicated team of cybersecurity professionals that performs tests in an attempt to "hack ourselves" on a scheduled and on-going basis. The penetration testing process provides the Agency with a third layer of defense beyond our basic cyber hygiene practices of software patching and vulnerability scanning.

This program includes both overt and covert penetration tests, utilizing real-world scenarios. We continually evolve our penetration-testing program as new threats emerge. We track, monitor, and remediate all identified vulnerabilities. Further, we scan all public facing applications for vulnerabilities prior to releasing them to production. We leverage the responses to regularly scheduled exercises and tests to mature the posture and performance of our Security Operations Center.

We also work with outside auditors and provide them access to our systems if requested to perform independent testing. We remediate the vulnerabilities identified by the independent auditor, and we actively detect and remediate additional vulnerabilities both internally and externally. It is important to note that auditors have had no success in breaking into our systems from the outside.

Malware and Anti-Phishing Defenses: The Agency defenses for malware and phishing are a critical component of our cybersecurity program and build on our layers of defense and risk based approaches. We take a holistic approach, incorporating malware and phishing defenses into the various layers of protections at the perimeter, network, end-point, data, prevention, and response layers. We deploy a variety of technologies to detect potentially malicious activity at our gateways to the external world as well as within our internal network. We configure our infrastructure and place controls on user activity to limit the impact of potentially suspicious actions. Some specific best practices are:

- The deployment of multiple technologies to automatically detect and remediate known malicious software at the virtual entry points into our infrastructure.
- The early adoption and continued upgrade of our Trusted Internet Connection and the deployment of the DHS Einstein program to identify malicious traffic targeting SSA and prevent it from harming us.
- The implementation of an enterprise wide social engineering program that tests our employees' ability to recognize suspicious email messages and phone calls. We test all employees once a quarter with phishing exercises to continuously reinforce their skills.

Authentication for *my* Social Security: As the Acting Commissioner mentioned in her testimony, SSA has a robust set of on-line services for citizens to use to conduct Social Security business. We have offered a multi-factor authentication method for citizens to use to access services since fiscal year 2012. This summer, we will make multi-factor authentication mandatory for users. All customers must enter a username, password and a one-time passcode texted to a registered cell phone in order to access their *my* Social Security account. This will ensure that the Agency on-line portal is consistent with the CyberSecurity Act of 2015, the

National CyberSecurity Action Plan, and Executive Order 13681. We are working with NIST and other Federal agencies to identify improvements to the authentication process.

FISMA Compliance and Performance

FISMA mandates that we implement an effective information security program and requires us to regularly assess our major IT systems and report the assessment results in an annual report to OMB and Congress. Our defense-in-depth cybersecurity program ensures that we manage information security risks on a continuous basis, as directed by OMB. In a network of our size and complexity, something can always be better secured. In accordance with FISMA requirements, an independent auditor evaluates our information security program and systems annually. Over the years, these evaluations have found us to be in compliance with the law, but like any audit, have identified areas for improvement.

Our inspector general (IG) contracted with an independent auditor to complete the FY 2015 FISMA audit. The evaluation determined that we established an information security program and practices that were generally consistent with FISMA requirements. However, our overall score was lower than FY 2014. In June 2015, the scoring metrics used by the IG to calculate our FISMA score changed. In total, 21 individual metrics were eliminated—in each of which we had a passing score in FY 2014. This change in scoring methodology contributed to an overall decline in Federal agency scores. With the new methodology, we ranked sixth out of 24 CFO Act agencies with an overall score of 84 points. This year, the methodology will change in another area. FISMA scores will continue to reflect changes to the methodology. Agencies may need time to understand the new methodology and improve effectiveness based on these changes.

The majority of our reduced compliance metrics fell into the area of Risk Management. Throughout the evaluation, we engaged the auditor to explain our approach, provide documentation of our progress, and obtain feedback on their assessment. The auditor noted in FY 2015 that we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources. We also improved our existing controls and implemented new controls and risk management processes in FY 2015. We completed actions on many recommendations from the FY 2014 and FY 2015 FISMA assessments and continue to address open recommendations.

In response to our auditor’s findings and recommendations, we expanded our penetration-testing program to include the analysis of external threats in addition to internal threats. We implemented a zero tolerance policy for weak credentials as we further refine our threat and vulnerability management program. We continue to emphasize prioritization and implementation of risk mitigation strategies and plans of action and milestones as we remediate vulnerabilities.

We continue to improve and standardize governance processes for IT applications within the agency. We established improved criteria for assessing the risk and security of applications. These steps help ensure our risk management requirements are effectively and consistently implemented across the organization. This includes our State DDSs, where we are accelerating

the expansion of our suitability clearance process. We also implemented an automated, standardized DDS security plan template that each DDS completed. Given our competing needs and limited resources, we follow best practices and prioritize our actions for improvement to address the most significant risks first.

Conclusion

Again, thank you for the opportunity to testify about these important issues. To summarize our IT security program, I will reiterate that we have a holistic, integrated, defense-in-depth program that ensures we practice good cyber hygiene through constant patching, monitoring, scanning, alerting, and awareness training. While continuing these basic practices, we must constantly add new layers of technology and automation to reduce our reliance on outdated manual processes.

As the threat level evolves and escalates, all organizations must respond with newer and innovative defenses that will improve our ability to respond quickly. Our future cyber program will include the use of more analytics tools to identify threats faster and the use of automation to respond and remediate incidents more quickly.

We have increased the amounts that we expend on cybersecurity programs over the last three fiscal years. However, our resources are constrained, and we need adequate resources and funding to maintain and improve our vitally important cyber defenses and protect the PII of all of our citizens.

Thank you and I am happy to answer any questions.

Marti Eckert
Chief Information Security Officer
Social Security Administration

Marti Eckert is the Chief Information Security Officer (CISO) at the Social Security Administration (SSA), where she is responsible for the Agency's Cyber Security Program, ensuring the protection of the Agency's vast information technology resources.

A career federal employee, Marti has held various Information Technology executive positions at Social Security. She led the implementation of Social Security's Business Services On-line suite of Internet applications which employers use to interact with Social Security. In 2006, she became the Deputy Associate Commissioner for the Office of Systems Electronic Services where she continued to lead the implementation of Social Security services on the Internet. In 2008, Marti made the switch from software development to hardware operations when she became the Assistant Associate Commissioner for Enterprise Information Technology Operations and Security where she was responsible for running Social Security's day to day data center operations.

Before becoming the SSA CISO in 2013, Marti was the Deputy Associate Commissioner for Telecommunications and Systems Operations. Marti holds a B.A. degree in political science from the University of Dayton and an M.B.A. degree from Loyola University.