United States House of Representatives

Committee on Oversight and Government Reform

Statement for the Record

Social Security Administration: Information Systems Review

Gale Stallworth Stone
Deputy Inspector General
Social Security Administration

Good morning, Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee. Thank you for the invitation to testify today, to discuss the Social Security Administration's (SSA) information security management and information technology investments.

The Office of the Inspector General (OIG) for many years has placed oversight of SSA's information technology infrastructure among its top priorities. During my tenure in the OIG's Office of Audit, I directed and oversaw our financial and information technology audits of SSA's operations, and I have served on the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board, so I appreciate the opportunity to discuss these critical issues with your Committee.

Protecting Government Information Systems

Government information systems, and the data they hold, are increasingly becoming targets of cyber attacks. Recent data breaches at government agencies have underscored the need for Federal agencies to make every effort to secure and protect sensitive information. In recognition of the rapidly increasing importance of government cybersecurity, Congress passed the *Cybersecurity Act of 2015.*[1]

It should come as no surprise that SSA—like other Federal agencies that collect and store voluminous amounts of personal information—could be a potential target for a cyber attack. The Agency houses sensitive information for nearly every U.S. citizen—living and deceased—including individual medical and financial records. SSA maintains 14 general support systems and 8 major applications to conduct its business, and it has tens of thousands of employees interacting with citizens in more than 1,200 field offices across the country.

While it is undoubtedly a significant and ongoing challenge to maintain uniform information security protocols across an organization as vast and complex as SSA, it is a challenge that must be met and remain a chief concern to Agency leadership and the OIG. Inappropriate and unauthorized access to, or theft of, SSA data could result in severe harm and distress to potentially hundreds of millions of Americans.

Last year, SSA provided about $930 billion in payments to about 67 million Americans; almost all of these transactions are electronic, and SSA encourages its customers to interact with the Agency though online services to apply for benefits, to input and edit direct deposit information, or to request a replacement Social Security card, for example. As it conducts more business online, SSA must ensure that it properly authenticates customers and secures transactions.

The *Federal Information Security Modernization Act of 2014* (FISMA) requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the data and systems that support the agency's operations and assets. The law also requires inspectors general to evaluate its agency's information security programs and practices on an annual basis, to include internal and external penetration testing of agency systems.

My statement will focus on the results of our most recent report on SSA's compliance with FISMA, though we have conducted many other reviews on SSA's information technology infrastructure, such as

[1] The law, among other things, established a voluntary framework for the sharing of cybersecurity threat information between and among the federal government, state governments, and private entities.

authentication and security controls over its electronic services, as well as SSA's major information technology investments, like the National Support Center and the Disability Case Processing System.

SSA's FISMA Compliance

In our most recent report on SSA's compliance with FISMA, we determined that SSA had established an information security program and practices that were generally consistent with FISMA requirements. However, we identified a number of deficiencies that may limit the Agency's ability to protect the confidentiality, integrity, and availability of SSA's information systems and data.[2] The deficiencies identified are consistent with those that we have cited in prior reports on SSA's FISMA compliance.

Before I review the reporting metrics that revealed significant deficiencies in SSA's information security controls, I want to highlight the importance of the Agency's efforts to implement NIST's Information System Continuous Monitoring (ISCM) strategy. Continuous monitoring helps organizations maintain ongoing awareness of information security, vulnerabilities, and threats to support risk-management decisions. ISCM calls for organizations to implement tools and processes that maintain situation awareness of all systems; maintain an understanding of threats and threat activities; assess all security controls; collect and analyze security-related information; and communicate security status across the organization.[3]

We reported that SSA has "defined" its ISCM strategy, but the Agency continues to rely on manual and procedural information-security methods in situations where automation may be more effective. ISCM requires active risk management by organizational officials, and it is most effective when automated, however we recognize that many aspects of the strategy, especially for legacy data systems as entrenched and complex as SSA's, are not easily automated. SSA's commitment to implementing a comprehensive ISCM strategy—to provide ongoing security monitoring and updates—is of critical importance. Considering the current threat of cyber attacks facing government agencies, a thorough continuous-monitoring program is necessary in any information security system.

Of the 10 FISMA reporting metrics, we cited significant deficiencies for SSA in configuration management, identity and access management, risk management, and security training.

Configuration Management

We identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner. I should note that, because disclosing specific details about these weaknesses in a public venue might further compromise controls, we provided those details to SSA management in a limited-distribution letter separate from our report.

Related to this issue, in a separate review of SSA's patch-management process, we found the Agency did not have a comprehensive patch program, thus it did not always address known vulnerabilities timely. Without an effective patch-management process, to include clear policies and procedures and assigned roles and responsibilities, SSA's systems are at risk of unauthorized access.[4]

---

[2] Under a contract the OIG monitored, an independent certified public accounting firm audited SSA's compliance with FISMA for fiscal year 2015. The OIG was responsible for technical and administrative oversight of the contractor's review.

[3] NIST, *Information Security Continuous Monitoring for Federal Systems and Organizations*, September 2011.

[4] SSA OIG, *Effectiveness of the Social Security Administration's Server Patch Management Process*, September 2014.

Identity and Access Management
We identified numerous issues with logical access controls that resulted in inappropriate and/or unauthorized access to information systems; this included programmers with unmonitored access to production and application transactions, as well as other users with inappropriate access to privileged functions and sensitive system software. Additionally, we identified control failures related to removing terminated employees' access to SSA's network and other systems, and the Agency was unable to track the departure dates for contractors and substantiate the removal of their systems access.

Risk Management
Weaknesses for information system controls for various non-central office sites continue to persist from past FISMA reviews because SSA has not designed, planned, or implemented corrective actions to remediate weaknesses and mitigate risks. These weaknesses include inadequate platform security, inadequate policy/procedural guidance, and inadequate development and implementation of a risk management framework.

Contributing factors to these weaknesses include SSA's lack of a comprehensive governance structure and an organization-wide risk management strategy; an inconsistent implementation of SSA's information security program requirements; and a lack of sufficient IT assessments performed by management.

Security Training
While SSA has established a security-training program that is consistent with FISMA requirements, the Agency does not have an authoritative system to identify and track the completion of security awareness training for employees and supervisors, including those with significant information security responsibilities.

Agency Efforts, OIG Recommendations
In our review of SSA's overall information security program and practices, we concluded that the risk and severity of the weaknesses described constituted a significant deficiency in internal controls over FISMA.[5] SSA has continued to pursue a risk-based approach to information security, and as I mentioned, the issues we found were similar to those we cited in prior reports on SSA's FISMA compliance.

These weaknesses continue to exist, we believe, because of one, or a combination, of the following:
- SSA's risk-mitigation strategies and related control enhancements require additional time to implement or become fully effective.
- SSA has focused resources on higher-risk weaknesses, and thus it is unable to take corrective actions on all prior-year deficiencies.
- Newly designed controls did not completely address the risks and recommendations provided in past reports.
- Information technology oversight and governance were not sufficient.

SSA should make all efforts to address the weaknesses identified. We also made several additional recommendations to the Agency, including:

[5] SSA OIG, *The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015*, November 2015.

- Continue, as part of the threat and vulnerability management process, to prioritize and implement risk mitigation strategies.
- Analyze account-management controls to determine whether the controls mitigate the risk of unauthorized access, and consider automating the account-management process.
- Continue, as part of the Cybersecurity Sprint initiative, to improve controls over privileged accounts.[6]
- Enhance current information technology oversight and guidance to ensure processes are effectively and consistently implemented across the Agency.
- Improve tracking of completion of security awareness training, especially for employees and contractors with significant information security responsibilities.

As FISMA requires, we will continue to assess annually the effectiveness of SSA's information security policies, procedures, and practices.

Authenticating Electronic Services Users

It is equally important that SSA ensure that it has controls in place and properly authenticates its electronic services users, as the Agency offers many of its customer service functions online, including benefit payment delivery through direct deposit.

Through SSA's *my* Social Security account, citizens now have the ability to update their personal records and access their benefit payment information with SSA online. SSA introduced the online account in 2012, and today more than 24.6 million people have registered accounts with the Agency.

In 2013, SSA enhanced *my* Social Security, allowing Social Security beneficiaries to change their mailing address or direct deposit bank information online. Around the time of this change, we began receiving reports of changes to beneficiary address and direct deposit information that beneficiaries did not make or had not authorized.

Since then, we have investigated many cases involving the fraudulent redirection of Social Security benefits through *my* Social Security accounts to financial accounts controlled by identity thieves. In one example, as the result of an OIG investigation with IRS Criminal Investigations and the FBI, a Miami man was sentenced in 2014 to 88 months in prison for using victims' personal information to create more than 900 fraudulent *my* Social Security accounts and then redirect about $700,000 in Social Security payments to bank accounts he controlled.

As this example shows, this is a serious issue, because electronic fraud schemes can affect a significant number of unknowing victims and lead to large Social Security fraud losses; additionally, electronic fraud cases are difficult to investigate, because the perpetrators can carry out this theft from computers or other devices anywhere in the world. In a recent report, we estimated that about $20 million in Social Security benefit payments to about 12,000 beneficiaries was redirected between January 2013 and January 2014; of that amount, about $11 million had not been returned to SSA, as of August 2015.[7]

[6] In June 2015, the Federal Chief Information Officer, through the Cybersecurity Sprint initiative, instructed agencies to implement a number of immediate high-priority actions to enhance the cybersecurity of Federal information and assets.

[7] SSA OIG, *Unauthorized Direct Deposit Changes through my Social Security*, September 2015.

SSA has improved its controls over *my* Social Security by strengthening the account registration process, establishing a fraud analysis team to investigate potential theft cases, and providing fraud awareness training to employees; we continue to review how the Agency safeguards *my* Social Security accounts and beneficiary information.

When notified, SSA generally moves quickly to resolve issues related to account and direct deposit information. However, given the sensitivity of the personal and financial information contained in *my* Social Security accounts—and the hardship that identity theft can cause—SSA reports it is planning to implement additional user authentication techniques to further guard against identity and benefit theft. We also continue to work closely with SSA to encourage citizens to protect their personal information, establish their own *my* Social Security account before identity thieves fraudulently do so, and regularly monitor their accounts for any suspicious activity.

SSA's IT Investments

SSA's spending on information technology in FY2016 totals $1.5 billion, according to the Office of Management and Budget's IT Dashboard; about 65 percent of those funds are dedicated to operations and maintenance; 32.5 percent are dedicated to development, modernization and enhancements; and the balance to provisioned services. The Agency is currently managing 14 "major" investments, including the National Support Center (NSC) and the Disability Case Processing System (DCPS). We have monitored both projects closely, as the projects' successful implementation is critical to SSA operations.

National Support Center

SSA is currently migrating systems from the National Computer Center (NCC) in Woodlawn, Maryland to the new NSC in Urbana, Maryland. The systems moving from the NCC to the NSC contain demographic, wage, and benefit information for almost every American, and the data are essential for SSA to provide its services to its customers.

SSA built and partially equipped the NSC to replace the aging NCC with $500 million provided by Congress in FY2009 under the *American Recovery and Reinvestment Act*. The NSC is a modern, efficient data center that is expected to meet the Agency's information technology needs for at least 20 years. SSA also operates the Second Support Center in North Carolina, which provides data computing redundancy.

The Agency is on schedule to complete systems migration to the NSC in August 2016. SSA and the General Services Administration have successfully managed this significant project thus far. To date, we have not identified any significant issues that would delay migration efforts; however, a seamless transition of data management to the NSC is critical to SSA operations. The Agency should continue to monitor the risks associated with data migration efforts until the process is complete; going forward, it should maintain appropriate data security plans, disaster recovery plans, and access management controls.[8]

Disability Case Processing System

State disability determination services (DDS) evaluate disability claims and make disability determinations for SSA; there are 54 DDSs across the country, and they use various customized systems to process disability claims.

[8] SSA OIG, *Progress Report on the Social Security Administration's National Support Center*, August 2015.

SSA envisioned DCPS as a singular tool for case processing for the DDSs, which SSA believed would simplify system support and maintenance, improve the speed and quality of the disability process, and reduce the overall growth rate of infrastructure costs. SSA launched the project in late 2010 and used an iterative approach to implement DCPS, starting at one test site and expanding to other test sites as functionality evolved.

In March 2014, SSA contracted with a consultant to analyze the project; in June 2014, the consultant reported that SSA invested $288 million in DCPS over six years, but the project delivered limited functionality and faced schedule delays amid increasing stakeholder concerns. SSA continued development and considered several options to complete the project, including whether off-the-shelf software or a modernized version of SSA's software could be integrated into DCPS. At the request of Congress, we followed up on the contractor's report and responded to several questions about the project. In November 2014, we issued a report and recommended that SSA suspend DCPS development while it evaluated project alternatives.[9]

SSA disagreed and continued developing DCPS, but due to coding and design issues, DCPS functionality remained incomplete. In May 2015, SSA decided to discontinue development and later "reset" the project and changed its technical approach. Teams made up of SSA staff and vendors began redeveloping the system and are currently working in an "agile" environment, which emphasizes collaboration between developers and business experts to incrementally deliver software. SSA's goal is to deliver the first release of the new DCPS system to some—but not all—DDSs by the end of December 2016. However, this "core" release will require DDSs to run parallel systems until SSA develops additional functionality and designs specific customization for many State agencies. State-specific customization proved to be the most complex task in SSA's previous attempt to design DCPS. Accordingly, we have significant concerns regarding the total cost of implementing this system, which, by the time the first release is made available, will total almost $500 million.

We acknowledge that DCPS still has the potential to provide significant value to SSA, but thus far, the project has proven to be very challenging. We continue to monitor DCPS and we will soon issue reports on development costs incurred and SSA's analysis of alternative solutions. Going forward, DCPS needs diligent oversight from Agency management and requires unified strategic decisions.

Conclusion

It is imperative that SSA continues to make protecting its networks and information a top priority; without updated, continuous security, its systems and the sensitive data they contain are at risk. The Agency should continue to dedicate resources to ensure the appropriate design and operating effectiveness of information security controls and prevent unauthorized access to the sensitive information the American public entrusts to SSA.

SSA must also maintain strong authentication controls to ensure that only SSA customers can access online accounts connected to individual personal information and benefit records. Finally, SSA must ensure it properly manages major information technology projects and delivers projects on budget and on time.

[9] SSA OIG, *The Social Security Administration's Disability Case Processing System*, November 2014.

Oversight of SSA's systems security is a top priority for the OIG. We will continue to monitor these and related issues closely and will work with SSA and the Committee on Oversight and Government Reform to enhance the Agency's information technology security and capabilities, so it can improve operations and serve its customers effectively. Thank you again for the invitation to testify, and I am happy to answer any questions.