United States House of Representatives

Committee on Ways and Means

Subcommittee on Social Security

Statement for the Record

The State of Social Security's Information Technology

Gale Stallworth Stone
Acting Inspector General
Social Security Administration

Good morning, Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee. Thank you for the invitation to testify today, to discuss the Social Security Administration's (SSA) information technology (IT) modernization, management, and security.

The Office of the Inspector General (OIG) for many years has placed oversight of SSA's IT infrastructure and information security practices among its top priorities, so I appreciate the opportunity to discuss these critical issues with your Subcommittee.

Background on SSA's IT Profile

Last year, SSA paid about $1 trillion to about 70 million Americans; almost all of these transactions are electronic, and SSA encourages its customers to interact with the Agency through various online services. SSA also houses sensitive information for nearly every U.S. citizen—living and deceased—including individual medical and financial records.

Given SSA's significant and increasing service and data-storage responsibilities, SSA must modernize its IT infrastructure to support current and future workloads. SSA's IT environment includes hundreds of applications and an array of technologies. To process its core workloads, such as retirement and disability claims, the Agency relies on decades-old applications programmed with Common Business Oriented Language (COBOL). SSA maintains more than 60 million lines of COBOL today, along with millions more lines of other legacy programming languages.

Additionally, as SSA experiences workforce turnover, employee knowledge of, and ability to work with, older technologies diminishes. SSA's next generation of employees will expect to work with current, mainstream technologies, such as open-source databases and cloud computing.

It is a significant challenge to enhance the databases, applications, and infrastructure that an organization as vast and complex as SSA needs to conduct business, but it is a challenge that Agency leadership must meet. The need for long-term IT planning has been a major concern for SSA for many years. As far back as 1982, SSA announced a Systems Modernization Plan to restructure and extensively upgrade its systems. At that time, the Agency told Congress that, without this major upgrade, there might be a serious disruption of its services, which are essential to millions of Americans. Despite progress in modernizing many of its systems since then, the Agency has yet to tackle some of its most complex and critical IT projects.

In implementing its modernization efforts, it is critical that SSA follow a well-planned IT roadmap that clearly outlines how it will enhance its data, applications, and infrastructure. Additionally, SSA must incorporate strong security measures in these new initiatives. In doing so, SSA will ensure Agency employees can work effectively and SSA customers can receive timely, accurate, and secure services.

My statement will focus on SSA's IT modernization and information security efforts, and I will discuss the OIG's monitoring of the Disability Case Processing System (DCPS), one of SSA's major IT investments.

SSA's IT Modernization Efforts

According to the Office of Management and Budget's IT Dashboard, SSA's spending on information technology in Fiscal Year 2018 totals $1.6 billion; SSA has six major IT investments, including IT modernization.

In October 2017, SSA issued its IT Modernization Plan, which outlined a multi-year effort to update SSA's major systems using modern architecture, Agile software engineering methods, cloud provisioning, and shared services. In the plan, SSA said it would invest $677 million over five years to support various modernization efforts.

SSA developed the plan with the following six goals: improve service to the public; increase the value of IT for business; improve IT workforce engagement; improve business workforce engagement; reduce IT and other operating costs; and reduce risk to the continuity of operations.

To achieve these goals, SSA identified eight major domains for modernization: Communications; Disability; Title II; Title XVI; Earnings; Enumeration; Data Modernization; and Infrastructure Modernization.

The OIG for many years has said that any IT modernization effort at SSA should be part of a long-term comprehensive strategic plan, so this strategy by SSA is a step in the right direction. As it nears the end of the first year of its five-year plan, the Agency recently reported it is redesigning its core programmatic business processes, the technology that underlies them, and the methods SSA uses to develop them.

This is a significant, but necessary undertaking, which will require close monitoring and management. We plan to formally evaluate SSA's IT modernization efforts next year.

Disability Case Processing System

While SSA embarks on these modernization efforts, DCPS development continues. SSA envisioned DCPS as a national, common case-processing system for State disability determination services (DDS), which evaluate disability claims and make disability decisions for SSA. There are 54 DDSs across the country, and they use various customized systems to process disability claims.

SSA conceived of DCPS in 2008 and expected it would simplify system support and maintenance, improve the speed and quality of the disability process, and reduce the growth of infrastructure costs. However, in March 2014, amidst schedule delays and stakeholder concerns, the Agency hired a consultant to provide an in-depth analysis of the project. In June 2014, the consultant reported that after almost six years of development, DCPS still delivered limited functionality. At the consultant's recommendation, SSA performed proof-of-concept evaluations of two other alternatives, including whether off-the-shelf software or a modernized version of SSA's existing software could be integrated into DCPS.

At the request of Chairman Johnson, we followed-up on the consultant's report and responded to several questions about the project. In November 2014, we recommended that SSA suspend DCPS development

while it evaluated these other project alternatives.[1] In May 2015, SSA decided to discontinue DCPS development and later "reset" the project with a new technical approach. Teams of SSA staff and vendors began redeveloping the system in an Agile environment, which emphasizes collaboration between developers and business experts to deliver software incrementally.

Before the Agency "reset" DCPS in 2015, SSA spent $356 million on DCPS development, an investment from which the Agency will receive little benefit.

When SSA altered its development approach, Chairman Johnson requested that we issue ongoing reports on SSA's progress in developing DCPS. In May 2016, we examined SSA's analysis of alternatives for DCPS and concluded that SSA did not fully analyze all potential alternatives, including whether to discontinue all efforts entirely and continue maintaining its legacy systems.[2]

Based on a request from Chairman Johnson and Chairman Orrin Hatch of the Senate Finance Committee, in April 2017, SSA hired a contractor to conduct market research and analyze SSA's options to deliver a common system to meet the Agency's disability case-processing requirements; the contractor considered three options: the current version of DCPS; a commercial off-the-shelf case-management system; and a modernized version of the vendor-owned existing systems used by the majority of DDSs. In July 2017, the contractor concluded that the current version of DCPS would best meet the Agency's requirements, and SSA leadership decided to continue DCPS development.[3]

SSA delivered the first release of the new DCPS to a few DDSs at the end of 2016 and the beginning of 2017. By September 2017, employees in 10 DDSs were using DCPS to process some of their disability workloads. At that time, we reported that SSA was working to deliver functionality in DCPS to support all initial and reconsideration cases by January 2018, and all remaining workloads—including continuing disability reviews and DDS disability hearings—by April 2018. The Agency was also planning to deploy a completed DCPS to all DDSs by September 2019 and retire all legacy systems by the end of Fiscal Year 2020.

However, in November 2017, SSA discontinued rolling out DCPS to additional DDSs and focused on system development. In March 2018, we reported that SSA's revised strategy focused on increasing the number of DCPS users at participating DDSs and the number of cases they process in the system.[4]

In July of this year, we issued a report that included survey results of 120 DCPS users. About 60 percent agreed or strongly agreed with the statement, "Overall, I am satisfied with DCPS." In general, users reported they liked the system's modern interface, ease of use, and the ability to work on multiple cases at once; they added that they would like to see additional functionality in the system.

---

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

[2] SSA OIG, *The Social Security Administration's Analysis of Alternatives for the Disability Case Processing System*, May 2016.

[3] SSA OIG, *Contractor's Market Research and Analysis for the Disability Case Processing System*, February 2018.

[4] SSA OIG, *Progress in Developing the Disability Case Processing System as of February 2018*, March 2018.

In that same report, we noted that in May 2018, the 10 participating DDSs completed 1,543 cases in DCPS, or about 4 percent of their workload. SSA did not establish goals for DCPS use at participating DDSs. Rather, SSA gave DDS administrators the discretion to determine the number of employees who would use the system and the types of volumes of cases they would process in it. SSA recognized that its inability to convince DDS users of the value and advantage of DCPS may negatively affect DDS adoption rates. To address this, the Agency planned to continue working with users to develop and demonstrate working software.

At the time of our May 2018 report, SSA was tentatively planning to resume deploying DCPS to additional DDSs in October 2018.[5] At this time, SSA plans to deploy DCPS to the majority of DDSs by December 2019.

Since SSA "reset" DCPS development in May 2015, SSA has spent $101 million on the project. The Agency anticipates spending an additional $76 million through Fiscal Year 2022, bringing the total estimated cost for this second DCPS attempt to $177 million. Additionally, SSA has estimated that the annual cost of maintaining the legacy systems is $32 million.

SSA's new version of DCPS has been implemented at more DDSs than the previous iteration, and it is showing more promise than the prior attempt. But while the estimated cost of the new DCPS is about half of what SSA spent on the previous effort, the Agency still faces risks that might increase costs and affect its ability to implement this new system nationwide.

Also, SSA has not identified the level of effort required to develop and deliver all the functionality DDSs need to fully process all their workloads. Each state has unique requirements to process payments, and complicated interface requirements could delay SSA's ability to deliver functionality and make maintaining those interfaces difficult. Furthermore, until SSA completes DCPS development and implementation, DDSs will continue incurring costs to operate and maintain their existing systems. These uncertainties may negatively affect the Agency's delivery timeline and costs.

SSA's Information Security

As SSA pursues its IT modernization goals, the Agency must also ensure the security of its information systems. Data breaches at government agencies have underscored the need for Federal agencies like SSA to make every effort to secure and protect information systems. In 2016, we stated that securing information systems and protecting sensitive data was a major management challenge facing SSA. We have issued several audit reports in this issue area.

For example, through SSA's *my* Social Security online account, a registered and authenticated user can access their benefits verification letter, payment history, and earnings record; change an address; input or change direct deposit information; and, in some cases, request a replacement Social Security number card. In 2016, we evaluated SSA's process for preventing unauthorized access to *my* Social Security accounts and ensuring it safeguards citizens' personally identifiable information, and we recommended that SSA implement appropriate authentication and identity proofing technology to *my* Social Security.[6]

---

[5] SSA OIG, *Use of the Disability Case Processing System as of May 2018*, July 2018.

[6] SSA OIG, *Access to the Social Security Administration's my Social Security Online Services*, September 2016.

SSA implemented two-factor authentication to the *my* Social Security portal in June 2017, but we believe the Agency should improve its identity verification controls to ensure users are who they claim to be.

Further, SSA manages a number of additional web applications to conduct business with the public, government agencies, and others. Hackers attempt to exploit any vulnerabilities in these types of applications to gain access to networks, so it is imperative that SSA identify these vulnerabilities and remediate them timely. We reviewed SSA's efforts to identify, assess, and remediate vulnerabilities in these applications and found that SSA could strengthen its controls over these security functions. In November 2016, SSA began tracking all vulnerabilities identified in an application that triggers automatic notification to the appropriate systems owner.[7]

The *Federal Information Security Modernization Act* (FISMA) requires each Federal agency to implement an agency-wide program to provide information security for its data and systems. The law also requires inspectors general to evaluate its agency's information security programs and practices on an annual basis.

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 control deficiencies that may limit the Agency's ability to protect the confidentiality, integrity, and availability of SSA's information systems and data.[8] The deficiencies were identified in several domains—information security continuous monitoring; configuration management; identity and access management; risk management; security training; incident response; and contingency planning—and were consistent with those that we have cited in prior reports on SSA's FISMA compliance.

Based on these control deficiencies, we concluded SSA's overall information security program was "Not Effective," according to FISMA criteria.[9] Weaknesses continued to exist, we believe, because of one, or a combination, of the following:

- SSA's risk-mitigation strategies and related control enhancements required additional time to implement or become fully effective.
- SSA focused resources on higher-risk weaknesses, and thus did not take corrective actions on all prior-year deficiencies.
- New controls did not completely address the risks and recommendations in past reports.

SSA should make all efforts to address the weaknesses identified. We also made several additional recommendations to the Agency, which we have detailed in our most recent report on SSA's compliance

---

[7] SSA OIG, *Security of the Social Security Administration's Public Web Applications*, April 2017.

[8] Under a contract the OIG monitored, an independent certified public accounting firm audited SSA's compliance with FISMA for fiscal year 2017. The OIG was responsible for technical and administrative oversight of the contractor's review.

[9] SSA OIG, *The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2017*, October 2017.

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

SSA stated in its IT Modernization Plan that the Agency's Cybersecurity Program would apply to all of its modernization efforts, as well as the rest of SSA's IT environment. SSA would implement security and privacy controls into applications and IT environments and systems at the beginning of development, according to the plan.

Specifically, SSA said its cybersecurity would focus on several areas, including strengthening identity credential and access management; expanding continuous diagnostic and mitigation capabilities; modernizing integrity review processes; establishing a Cyber Defense Operations Center; and maintaining continuous cybersecurity risk management and governance.

Conclusion

It is imperative that SSA follow a plan to modernize its IT infrastructure. Continued reliance on legacy coding and applications is unsustainable in the long term, given SSA's increasing service and data-storage responsibilities. SSA must work toward adopting current, mainstream programing languages, software, and storage capabilities.

For many years, the OIG has recommended that SSA incorporate its IT development strategy into its long-term strategic planning process, so we are encouraged that the Agency developed and implemented an IT Modernization Plan in 2017. Still, as SSA works to reduce its reliance on legacy systems and convert to modern applications and cloud storage, these efforts will take significant management, monitoring, and resources.

Oversight of SSA's IT planning is a top priority for the OIG. We will continue to track these and related issues, and we will work with SSA and this Subcommittee to help the Agency enhance its IT capabilities and security, so SSA can improve operations and serve its customers effectively.

Finally, I must take this opportunity to commend Chairman Johnson as he concludes a decorated, distinguished career in service to his country. The Chairman served for 29 years in the United States Air Force, and he was a fighter pilot in both the Korean War and the Vietnam War, during which he overcame tremendous adversity as a prisoner of war from 1966 to 1973.

After his military career, he was elected to the Texas House of Representatives. In 1991, Chairman Johnson was elected to the U.S. House of Representatives, and he has represented Texas's third congressional district for more than 26 years. He has served as Subcommittee Chairman since 2011, and he has been unwavering in his commitment to improving Social Security, so the Agency can assist future generations of Americans who truly deserve and depend on its programs.

Thank you, Chairman, for your service, your sacrifice, and your leadership. I am happy to answer any questions.