

United States House of Representatives

Committee on Ways and Means

Subcommittee on Social Security



Statement for the Record

**Modernizing Social Security's
Information Technology Infrastructure**

Kimberly A. Byrd
Deputy Assistant Inspector General for Audit
Office of the Inspector General
Social Security Administration

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

The Office of the Inspector General (OIG) for many years has placed oversight of SSA's IT infrastructure among its top priorities. As the Deputy Assistant Inspector General for the OIG's Office of Audit, I direct and oversee our financial and IT audits of SSA's operations, so I appreciate the opportunity to discuss these critical issues with your Subcommittee.

Background on SSA's IT Profile

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 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, SSA's workforce, while extremely proficient and experienced, is aging, thus employee knowledge of, and ability to work with, older technologies is diminishing due to retirement. SSA's next generation of employees will expect to work with current, mainstream technologies, such as open-source databases and cloud computing.

While it is undoubtedly a significant and ongoing challenge to enhance the databases, applications, and infrastructure that an organization as vast and complex as SSA needs to conduct business, 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 the welfare of 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.

The OIG, for many years, has said that any IT modernization effort at SSA should be part of a long-term comprehensive strategic plan. SSA needs a detailed IT roadmap that clearly outlines how it will enhance its data, applications, and infrastructure so Agency employees can work effectively and SSA customers can receive timely, accurate services. While we do not know the content of SSA's newest modernization plan—as SSA is still drafting the plan—we do believe it is critical that the plan be long-term and fully developed.

My statement will focus on SSA's IT modernization efforts and relevant OIG audit work on these efforts, and I will discuss the OIG's oversight of the Disability Case Processing System (DCPS), one of SSA's largest active IT investments. Also, I will note that SSA's IT modernization plans and efforts, while critical, should not supersede a commitment to information systems security; information security efforts should be included in any long-term IT planning at SSA.

SSA's IT Modernization Efforts

SSA's spending on information technology in FY2016 totals \$1.5 billion, according to the Office of Management and Budget's (OMB) 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.

SSA recently reported to the OIG that the Agency's formal IT modernization plan is still in draft status, so the OIG has not received or reviewed a finalized plan from SSA, thus I am not in a position to comment on any new strategies the Agency may have recently planned. However, according to [SSA's Information Resources Management Strategic Plan](#) (FY2016-2019), the Agency has identified several multi-year efforts to update its data architecture and applications and deploy a cloud infrastructure. We have conducted various reviews on SSA's progress in these areas.

Data Modernization and Consolidation

SSA reported that it is executing a two-part strategy to connect its master data with contemporary technologies. The Agency said it would move its master data from legacy storage systems to a standard database platform, and it would examine the form of its master data, recognizing that the data should exist in forms that are widely used in modern IT applications and databases.

In 2010, we reported on SSA's efforts to convert its legacy file management system. At the time, we found that SSA had effectively implemented the project to replace its master database, however, the project implementation strategy was not efficient because the strategy resulted in less-than-optimal database design. We recommended that SSA establish a long-term, comprehensive strategic plan for the project and related major IT initiatives, and ensure it performed an analysis of alternatives for future major IT investments.¹

Application Modernization

SSA said it would use modern programming language in the development for all new and modernized applications. The Agency reports it plans to modernize its "line-of-business" application systems, including the Earnings and Wage Reporting, Retirement and Disability Benefit Management, Representative Payee, and Supplemental Security Income Management systems, with a goal to integrate modernized applications with SSA's online and mobile services.

Ideally, Social Security technicians could work with applications that provide immediate access to transactions that customers have conducted online or via mobile device. SSA said it wants to move away from monolithic, single-use applications, which have higher costs and limited flexibility.

In 2012, we reviewed SSA's reliance on COBOL to process its core workloads. Our review, at the time, determined SSA did not have a strategic plan to convert its legacy COBOL application programs to a more modernized programming language. Rather, the Agency developed and has continued what it calls an "opportunistic" approach to, gradually, reduce its reliance on COBOL to process its core program transitions. We also reported then that SSA's continued use of and reliance on COBOL affected its IT system environment and limited its potential modernization efforts.²

¹ SSA OIG, [Conversion of the Social Security Administration's Legacy File Management System](#), May 2010.

² SSA OIG, [The Social Security Administration's Software Modernization and Use of Common Business Oriented Language](#), May 2012.

Infrastructure

SSA said, after a 2015 pilot-use of a Linux server, SSA would undertake a multi-year project to migrate away from, and ultimately retire, its proprietary mid-tier UNIX servers to more flexible Linux servers.

SSA is also exploring how cloud computing can help the Agency conduct business. SSA's cloud strategy involves implementing and examining private cloud-computing models before it extends that capability to public service functions.

In 2014, we evaluated SSA's cloud computing technologies. We conducted the review early in SSA's cloud-adoption process, so we encouraged SSA to consult with OMB on Federal requirements for cloud use.³ SSA recently reported that the Agency's cloud implementations have complied with Federal Risk and Authorization Management Program security assessments.

SSA's IT Investments

The Agency is currently managing 14 "major" IT investments, including the National Support Center (NSC) and DCPS. We have monitored both projects closely.

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 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 IT 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. 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, SSA should maintain appropriate data security plans, disaster recovery plans, and access management controls.⁴

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.

SSA envisioned DCPS as a single 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. Since SSA conceived of this common processing

³ SSA OIG, [The Social Security Administration's Cloud Computing Environment](#), December 2014.

⁴ SSA OIG, [Progress Report on the Social Security Administration's National Support Center](#), August 2015.

system in 2008, SSA has invested over \$300 million in DCPS—for which the Agency will receive very little value.

In March 2014, the Agency hired a consultant to provide an in-depth analysis of the project. In June 2014, the consultant reported that although SSA had invested \$288 million in DCPS over six years, the project delivered limited functionality and faced schedule delays amid increasing stakeholder concerns. 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 software could be integrated into DCPS.

At the request of Chairman Johnson, 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 these other project alternatives.⁵ SSA disagreed and continued developing DCPS—spending another \$23 million on additional coding and design. This work was never rolled out to the test sites. 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 and are currently working in an “Agile” environment, which emphasizes collaboration between developers and business experts to deliver software incrementally.

SSA's goal is to deliver the first release of the new DCPS system to some—but not all—DDSs by the end of 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.

Further, we recently examined SSA's analysis of alternatives for DCPS after the consultant's report raised concerns about the project. We concluded that SSA did not fully analyze all potential alternatives, including whether to discontinue all efforts entirely and continue maintaining its legacy systems.

At the end of FY2015, SSA reported it spent \$355 million on DCPS (including the first year of its reset). SSA projected DCPS contract and development costs for FY2016 and FY2017 to be \$84 million, bringing the total estimated DCPS cost through FY2017 to \$439 million. Additionally, SSA estimated that the annual cost of maintaining the legacy systems until discontinuing use of these systems is \$32 million. SSA has not estimated costs beyond FY2017 to maintain and enhance DCPS. Going forward, DCPS needs diligent oversight from Agency management and continued user involvement.

Agile Development in DCPS

I mentioned that when SSA reset DCPS in 2015, the Agency decided to implement Agile development practices. Agile differs from the traditional “waterfall” development method, in that Agile calls for brief development “sprints,” with rounds of design, testing, and feedback to deliver incremental product updates. The waterfall model is more traditional, in that it is a sequential design process, flowing downward through the development phases of requirements, design, implementation, verification, and maintenance. With the waterfall method, a project, at some point, is considered “delivered” and “complete,” while with the agile model, development is ongoing, as tests and adjustments continue after the project is in use.

⁵ SSA OIG, [The Social Security Administration's Disability Case Processing System](#), November 2014.

The consultant that analyzed DCPS in 2014 recommended SSA consider the Agile development approach. Agile can speed project development and reduce costs, but the consultant cautioned that transitioning to a new development methodology mid-project carries risk, and that large-scale projects often face challenges despite implementing Agile.

SSA has sought Agile training and coaching services from industry experts; nonetheless, Agile software development practices are relatively new at SSA, and implementing them on a project as complex as DCPS could introduce additional risks to a project that has already encountered such significant costs and delivery delays.⁶ OMB issued draft performance measurement guidance on Agile in April; when the guidance is finalized, we will begin a review of SSA's use of Agile for DCPS.

SSA's Information Security

Any long-term plan SSA develops with regard to IT modernization also needs to address efforts to secure the Agency's information systems. Recent data breaches at government agencies have underscored the need for Federal agencies like SSA to make every effort to secure and protect information systems.

The *Federal Information Security Modernization Act* (FISMA) requires each Federal agency to implement an agency-wide program to provide information security for the agency's 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 deficiencies that may limit the Agency's ability to protect the confidentiality, integrity, and availability of SSA's information systems and data.⁷ The deficiencies identified in several FISMA reporting metrics—configuration management, identity and access management, risk management, and security training—are consistent with those that we have cited in prior reports on SSA's FISMA compliance.

In our review of SSA's overall information security program and practices, we concluded that the risk and severity of the weaknesses identified constituted a significant deficiency in internal controls over FISMA.⁸

SSA continues to pursue a risk-based approach to information security, and 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.

⁶ SSA OIG, [Congressional Response Report: The Social Security Administration's Analysis of Alternatives for the Disability Case Processing System](#), May 2016.

⁷ 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.

⁸ SSA OIG, [The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015](#), November 2015.

- SSA focused resources on higher-risk weaknesses, and thus it was unable to take corrective actions on all prior-year deficiencies.
- New controls do 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 with FISMA. As FISMA requires, we will continue to assess annually the effectiveness of SSA's information security policies, procedures, and practices.

Conclusion

It is imperative that SSA clearly define its plan to modernize its IT infrastructure. The Agency's increasing service and data-storage responsibilities require SSA to transition from legacy coding and applications to current, mainstream programming languages, software, and storage capabilities. SSA has general plans to, gradually, reduce its reliance on legacy systems and convert to modern applications and cloud storage, but these efforts will take significant planning, time, and resources, as well as careful oversight. The OIG, for many years, has recommended that SSA incorporate its IT development strategy into its long-term strategic planning process. Despite some progress by SSA to identify areas for modernization, the OIG has not reviewed a formal IT modernization plan from the Agency.

Oversight of SSA's IT planning is a top priority for the OIG. We will continue to monitor these and related issues closely and will work with SSA and this Subcommittee to enhance the Agency's IT capabilities and security, 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.