United States Government Accountability Office

Testimony

Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

SOCIAL SECURITY ADMINISTRATION

Effective Planning and Management Practices Are Key to Overcoming IT Modernization Challenges

Statement of Valerie C. Melvin, Director
Information Management and Technology Resources Issues

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee:

I am pleased to be here today to participate in your hearing on modernizing the Social Security Administration's (SSA) information technology (IT). SSA is responsible for delivering services that touch the lives of almost every American, and the agency relies heavily on IT resources to do so. Its computerized information systems support a wide range of activities—from processing Disability Insurance and Supplemental Security Income payments to calculating and withholding Medicare premiums and issuing Social Security numbers and cards. For fiscal year 2015, the agency reported spending approximately $1.3 billion on hardware and software, computer maintenance, and contractor support, among other things.

SSA has acknowledged the increasing age of its IT environment and has reported that some of its databases are at least 40 years old. Moreover, our recent reporting on federal agencies' legacy IT[1] has noted the increasing cost for agencies, including SSA, to operate and maintain their outdated systems. SSA has initiated various projects over the past two decades that were intended to update and improve parts of its infrastructure. More recently, it announced plans to pursue an agency-wide IT modernization initiative.

At your request, my testimony today summarizes results from a number of our previous reports on SSA's IT efforts. Additionally, in anticipation of the agency's planned modernization initiative, my testimony highlights selected best practices that we have identified as being essential to an agency's effective planning and management for such an initiative.

In developing this testimony, we relied on reports that we have previously issued. These reports, cited throughout this statement, include detailed information on the scope and methodology for our reviews. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions.

---

[1]GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

SSA's mission is to deliver Social Security services that meet the changing needs of the public. The *Social Security Act* and amendments[2] established three programs that the agency administers:

- *Old-Age and Survivors Insurance*—provides monthly retirement and survivors benefits to retired and disabled workers, their spouses and their children, and the survivors of insured workers who have died. SSA has estimated that, in fiscal year 2017, $813 billion in old-age and survivors insurance benefits are expected to be paid to a monthly average of approximately 52 million beneficiaries.

- *Disability Insurance* provides monthly benefits to disabled workers and their spouses and children. The agency estimates that, in fiscal year 2017, a total of approximately $149 billion in disability insurance benefits will be paid to a monthly average of about 11 million eligible workers.

- *Supplemental Security Income* is a needs-based program financed from general tax revenues that provides benefits to aged adults, blind or disabled adults, and children with limited income and resources. For fiscal year 2017, SSA estimates that nearly $59 billion in federal benefits and state supplementary payments will be made to a monthly average of approximately 8.4 million recipients.

SSA relies on its IT resources to support the administration of its programs and related activities. For example, among other things, its systems are used to handle millions of transactions on the agency's website, maintain records for the millions of beneficiaries and recipients of its programs, and evaluate evidence and make determinations of eligibility for benefits. According to the agency's most recent *Information*

---

[2] Title II, *Federal Old-Age Survivors, and Disability Insurance*, and Title XVI, *Supplemental Security Income for the Aged, Blind and Disabled*, of the *Social Security Act* are administered by the Social Security Administration. See 42 U.S.C. §§ 401-434 and 42 U.S.C. §§ 1381-1383f.

Resources Strategic Plan,[3] its systems supported the processing of an average daily volume of about 185 million individual transactions in fiscal year 2015.

SSA's Office of the Deputy Commissioner for Systems is responsible for developing, overseeing, and maintaining the agency's IT systems. Comprised of approximately 3,800 staff, the office is headed by the Deputy Commissioner, who also serves as the agency's Chief Information Officer (CIO).

SSA's acting commissioner has stated that the agency's aging IT infrastructure is not sustainable because it is increasingly difficult and expensive to maintain. Accordingly, the agency has requested $300 million in its fiscal year 2017 budget to be spread over 4 years to modernize its IT environment. As reflected in the budget, these modernization efforts are expected to include projects such as updating database designs by converting them to relational databases, eliminating the use of outdated code, and upgrading infrastructure.

Among the agency's priority IT spending initiatives expected to be covered in the budget is its Disability Case Processing System. This system is intended to replace the 54 disparate Disability Determination Services'[4] component systems, support, and maintenance processes with a modern, common case processing system. According to SSA, the new system was to modernize the entire claims process, including case processing, correspondence, and workload management. However, SSA and others have reported substantial difficulty in the agency's ability to carry out this initiative, citing software quality and poor system performance as issues. Consequently, as of June 2016, the initiative had been placed on the Office of Management and Budget's government-wide list of 10 high-priority programs requiring attention.[5]

---

[3]SSA, *Social Security Administration Information Resources Management Strategic Plan 2016-2019* (Baltimore, Md.).

[4]SSA has agreements with state Disability Determination Services agencies to initially determine whether applicants are disabled.

[5]Office of Management and Budget, *Report to Congress: 10 High Priority Programs* (Washington, D.C.: June 9, 2016).

SSA Has Faced Long-Standing Challenges in IT Management and Modernization Efforts

We have issued previous reports highlighting various challenges in SSA's management of its IT. Overall, these reports identified weaknesses in, among other areas, system development practices, IT governance, requirements management, and strategic planning. Our reports, collectively, stressed the need for the agency to strengthen its IT management controls.

- In previously reporting on SSA's implementation of a new electronic disability system, we noted that the agency had proceeded without (1) conducting testing that was adequate to evaluate the performance of all system components collectively and (2) evidence that it had consistently applied established procedures to guide the system's development.[6] In view of the risks and the technological complexity, scope, and size of the initiative, we recommended that the agency, before continuing with its national rollout of the electronic disability system, ensure that all critical problems identified in pilot testing of the system were resolved and that end-to-end testing of the interrelated systems was performed; and ensure that all software that had been developed was approved and that systems were certified for production. SSA disagreed with the need for the end-to-end testing, stating that to perform such testing would delay the project and the agency's ability to realize benefits from this initiative. However, the agency did subsequently take measures to ensure that users approved new software and that it certified its systems for production.

- In an evaluation of SSA's investment management approach,[7] we noted that, while the agency had executed a majority of key IT investment management practices, the critical process of providing oversight was not being fully executed. Further, we reported that a gap existed in the agency's management of its IT in that more than half of its budget—for acquisitions—was not being overseen as part of the agency's investment management process. We made seven recommendations related to strengthening the agency's investment management capability. SSA agreed with six of our seven recommendations, and took actions to address five of them. For example, it established portfolio-level performance evaluation policies and procedures and criteria for assessing portfolio performance; it also tracked the status of corrective actions for underperforming IT

---

[6]GAO-04-466.

[7]GAO-08-1020.

projects. However, the agency did not implement post-implementation reviews and was not managing its acquisitions within its IT investment management framework. Further, the agency disagreed with our recommendation that it develop policies and procedures for managing its IT acquisitions as investments and manage them using the investment board and investment management processes. The agency disagreed because it believed its existing investment management framework was adequate. Given that IT product and service acquisitions made up the majority of SSA's IT budget, however, the investment board's involvement was essential to helping ensure effective management of and full accountability for these acquisitions.

- In previously reporting on SSA's efforts to ensure that its IT infrastructure can support the agency's future data exchange environment,[8] we noted that a detailed analysis needed to project the workload and performance requirements was not performed. In addition, we reported that the agency's target enterprise architecture environment did not address specific business and technical requirements for supporting its data exchange program. We recommended that SSA conduct the analyses needed to define requirements for delivering data exchange services to its partners in the future and use the results of these analyses to update its target architecture. SSA agreed with these recommendations and, in September 2013, took actions to address them. For example, it conducted an assessment of its existing electronic exchange architecture and identified challenges it expected to encounter as requests for data increased, as well as descriptions of target architectural components intended to meet requirements for addressing the challenges.

- In an examination of the agency's IT modernization approach, we pointed out that the approach lacked key practices to effectively guide its efforts.[9] Specifically, SSA did not have an updated IT strategic plan to guide its modernization efforts and its enterprise architecture lacked important content that would have allowed the agency to more effectively plan its investments. We recommended that SSA take four actions. For example, we recommended that in updating the IT

---

[8]GAO-09-966.

[9]GAO-12-495.

strategic plan to support the agency's strategic plan, SSA include key elements—such as results-oriented goals, strategies, milestones, performance measures, and an analysis of interdependencies among projects and activities—and use the plan to guide and coordinate IT modernization projects and activities. We also recommended that the agency establish an enterprise architecture plan that included key components called for by federal guidelines[10] and GAO's enterprise architecture management framework[11]—such as the development of a service-oriented architecture road map—to effectively guide its modernization activities. The agency neither agreed nor disagreed with our recommendations. However, it subsequently took action to address two of the four recommendations by ensuring that performance measures were defined for ongoing IT modernization initiatives and updating its IT strategic plan to support the agency's strategic plan. As of this testimony, we have not yet completed our evaluation of the agency's actions to address the other two recommendations related to establishing an enterprise architecture plan and developing and clearly documenting investment review guidance and procedures to ensure oversight reviews will be effective in evaluating and controlling investments.

Beyond the challenges identified in the aforementioned reports, our recent report on federal agencies' IT legacy systems highlighted the increasing costs that agencies, including SSA, may be faced with as they continue to operate and maintain at-risk legacy systems.[12] We identified SSA's investment in infrastructure operations and maintenance as being among the 10 largest expenditures of federal agencies in fiscal year 2015. Further, we pointed out that legacy systems may become increasingly more expensive as agencies have to deal with issues, such as obsolete parts and unsupported hardware and software, and may pay

---

[10]For example, Federal CIO Council, *A Practical Guide to Federal Service Oriented Architecture, version 1.1* (Washington, D.C.: June 2008); Office of Management and Budget (OMB), *Management of Federal Information Resources,* OMB Circular No. A-130 Transmittal Memorandum #4 (Washington, D.C.: Nov. 28, 2000); and OMB, *Information Technology Architectures,* Memoranda 97-16 (Washington, D.C.: June 18, 1997).

[11]GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, GAO-10-846G (Washington, D.C.: August 2010).

[12]GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

a premium to hire staff or engage contractors with the knowledge to maintain outdated systems. For example, SSA reported re-hiring retired employees to maintain its systems that include many programs written in Common Business Oriented Language (COBOL).

Our prior work further emphasized the importance of federal agencies using investment operational analyses—a key performance evaluation and oversight mechanism required by the Office of Management and Budget—to ensure operations and maintenance investments continue to meet agency needs.[13] We noted that SSA had not previously conducted this analysis for its investments. An analysis such as this is important because, among other things, it provides information to agency decision makers on whether an investment's actual annual operations and maintenance costs are as they were planned to be and whether there is a need to examine more cost-effective approaches to meeting agency mission objectives. We recommended that SSA perform such an analysis on its investment, and in January 2014 the agency did so.

Key Practices Are Essential for Managing Successful Modernizations

Our prior work has shown that effectively managing IT needs depends on federal departments and agencies, including SSA, having key processes in place.[14] Toward this end, we have identified and reported on a set of essential and complementary management disciplines that provide a sound foundation to support IT modernization efforts. These include the following:

- **Strategic planning:** Strategic planning defines what an organization seeks to accomplish and identifies the strategies it will use to achieve desired results. A defined strategic planning process allows an agency to clearly articulate its strategic direction and to establish linkages among planning elements such as goals, objectives, and strategies. A well-defined IT strategic planning process helps ensure that an agency's IT goals are aligned with its strategic goals.[15] Also,

---

[13]GAO, *Information Technology: Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance*, GAO-14-66 (Washington, D.C.: Nov. 6, 2013).

[14]GAO, *Library of Congress: Strong Leadership Needed to Address Serious Information Technology Management Weaknesses,* GAO-15-315 (Washington, D.C.: Mar. 31, 2015).

[15]GAO-12-495.

as part of its strategic planning efforts, an organization should develop an enterprise architecture, which is an important tool to help guide the organization toward achieving the goals and objectives in its IT strategic plan.[16] In addition, the organization should implement human capital management practices to sustain a workforce with the skills necessary to execute its strategic plan, which includes assessing current and future agency skill needs.[17]

- **IT investment management:** IT projects can significantly improve an organization's performance, but they can also become costly, risky, and unproductive. Agencies can maximize the value of these investments and minimize the risks of acquisitions by having an effective and efficient IT investment management and governance process, which would include instituting an investment board, selecting investments that meet business needs, providing investment oversight, and capturing investment information.[18] Emphasizing the importance of investment management, the *Clinger-Cohen Act* requires executive branch agencies to establish a process for selecting, managing, and evaluating IT investments in order to maximize the value and assess and manage the risks of the acquisitions.[19]

- **Systems development and acquisition:** Our prior reviews have shown that proper implementation of disciplined practices for developing or acquiring IT systems can significantly increase the likelihood of delivering promised system capabilities on time and

---

[16]GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0) (Supersedes GAO-03-584G)*, GAO-10-846G (Washington, D.C.: August 2010).

[17]Such practices have been identified by both the Office of Personnel Management and GAO. See Office of Personnel Management, *The Human Capital Assessment and Accountability Framework—Systems, Standards, and Metrics* (http://www.opm.gov/hcaaf_resource_center/) and GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003).

[18]GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity (Supersedes AIMD-10.1.23)*, GAO-04-394G (Washington, D.C.: March 2004).

[19]40 U.S.C. § 11312.

within budget.[20] These practices include defining the requirements that address the needs of the system users, managing project risk to identify potential problems before they occur, reliably estimating cost to help managers evaluate affordability and performance against a project's plans, and developing an integrated and reliable master schedule that defines when and how long work will occur and how each activity is related to the others, among other actions. Best practices in these areas have been identified by organizations such as the Software Engineering Institute and GAO.[21]

- **Information security and privacy:** Effective security for federal IT systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information, including personal information entrusted to the government by members of the American public. Recognizing the importance of information security and privacy, Congress enacted the *Federal Information Security Modernization Act of 2014*,[22] which requires executive branch agencies to develop, document, and implement an agency-wide information security program.[23] Additionally, in order to help agencies develop such a program, the National Institute of Standards and Technology has developed guidance for information security and privacy.

- **Service management:** Agencies should develop and implement a process for ensuring that IT services, such as server management and desktop support, are aligned with and actively support the business needs of the organization. The Information Technology Infrastructure Library[24] identifies key practices for successful service

---

[20]See, e.g., GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, GAO-12-7 (Washington, D.C.: Oct. 21, 2011).

[21]SEI, *CMMI® for Development and Acquisition, Versions 1.3*; GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C., March 2009); and GAO-16-89G.

[22]Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014).

[23]The *Federal Information Security Modernization Act of 2014*, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) partially superseded the *Federal Information Security Management Act of 2002*, enacted as Title III, *E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[24]Lou Hunnebeck and Colin Rudd, *ITIL: Service Design ©* (London: The Stationary Office, 2011).

management. These include developing a service catalog that identifies all IT services delivered by the service provider, as well as establishing service-level agreements between the IT service provider and its customer on the expected service-level targets.[25]

- **Leadership:** Effective leadership, such as that of a CIO, can drive change, provide oversight, and ensure accountability for results. Congress has also recognized the importance of having a strong agency CIO. For example, as part of the *Clinger-Cohen Act*, Congress required executive branch agencies to establish the position of agency CIO.[26] The act also gave these officials responsibility and accountability for IT investments, including IT acquisitions, monitoring the performance of IT programs, and advising the agency head on whether to continue, modify, or terminate such programs. More recently, in December 2014, Congress passed federal information technology acquisition reform legislation (commonly referred to as FITARA), which strengthened the role that agency CIOs are to play in managing IT.[27] For instance, the law requires the head of covered agencies to ensure that the CIO has a significant role in the decision process for IT budgeting, as well as the management, governance, and oversight processes related to IT.

In conclusion, given SSA's longstanding challenges with IT management and modernization efforts, it will be important for the agency to implement a clearly established, rigorous, and disciplined approach for its current efforts to manage and modernize its aging IT systems. Leveraging IT management best practices that we and others have identified and clearly documenting what is to be achieved, in what time frame, and at what cost could help position the agency to overcome challenges like those

---

[25]Examples of service-level targets include the hours that customers can expect the service to be available (e.g., 8:00 a.m. to 6:00 p.m., Monday through Friday), availability of a service during the agreed service hours (e.g., 99.5 percent), and maximum number of failures or incidents that can be tolerated within an agreed time period.

[26]Pub. L. No. 104-106, § 5125, 110 Stat. 186, 684 (Feb. 10, 1996); 40 U.S.C. § 11315 and 44 U.S.C. § 3506(a).

[27]*Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, Div. A, Title VIII, Subtitle D, § 831, 128 Stat. 3292, 3438 (Dec. 19, 2014); 40 U.S.C. § 11319.

encountered with past IT efforts. Without doing so, such challenges could continue to be an impediment to the agency achieving the more modernized IT environment that it needs.

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions that you or other members of the Subcommittee may have.

GAO Contact and Acknowledgments

If you or your staff have any questions about this testimony, please contact Valerie C. Melvin, Director, Information Management and Technology Resources Issues, at (202) 512-6304 or melvinv@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony statement. GAO staff who made key contributions to this statement are Nicole Jarvis (Assistant Director), Nancy Glover, Monica Perez-Nelson, Scott Pettis, and Christy Tyson (Analyst in Charge).