United States Government Accountability Office

Testimony

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

For Release on Delivery
Expected at 11:00 a.m. ET
Thursday, September 27, 2018

INFORMATION TECHNOLOGY

SSA Has Improved Acquisitions and Operations, but Needs to Fully Address the Role of Its Chief Information Officer

Carol C. Harris, Director, Information Technology Management Issues

September 2018

INFORMATION TECHNOLOGY

SSA Has Improved Acquisitions and Operations, but Needs to Fully Address the Role of Its Chief Information Officer

GAO Highlights

Highlights of GAO-18-703T, a testimony before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

Why GAO Did This Study

SSA delivers services that touch the lives of almost every American, and relies heavily on IT resources to do so. Its systems support a range of activities, such as processing Disability Insurance payments, to calculating and withholding Medicare premiums, and issuing Social Security numbers and cards. For fiscal year 2018, the agency planned to spend approximately $1.6 billion on IT.

GAO has previously reported that federal IT projects have often failed, in part, due to a lack of oversight and governance. Given the challenges that federal agencies, including SSA, have encountered in managing IT acquisitions, Congress and the administration have taken steps to improve federal IT, including enacting federal IT acquisition reform legislation and issuing related guidance.

This statement summarizes GAO's previously reported findings regarding SSA's management of IT acquisitions and operations. In developing this testimony, GAO summarized findings from its reports issued in 2011 through 2018, and information on SSA's actions in response to GAO's recommendations.

What GAO Recommends

GAO has made 15 recommendations to SSA to improve its management of IT acquisitions and operations from 2011 through 2018, and 1 recommendation to improve its CIO policies. While SSA has implemented nearly all of them, it would be better positioned to overcome longstanding IT management challenges when it addresses the CIO's role in its policies.

View GAO-18-703T. For more information, contact Carol C. Harris at (202) 512-4456 or harriscc@gao.gov.

What GAO Found

The Social Security Administration (SSA) has improved its management of information technology (IT) acquisitions and operations by addressing 14 of the 15 recommendations that GAO has made to the agency. For example,

- **Incremental development**. The Office of Management and Budget (OMB) has emphasized the need for agencies to deliver IT investments in smaller increments to reduce risk and deliver capabilities more quickly. In November 2017, GAO reported that agencies, including SSA, needed to improve their certification of incremental development. As a result, GAO recommended that SSA's CIO (1) report incremental development information accurately, and (2) update its incremental development policy and processes. SSA implemented both recommendations.
- **Software licenses**. Effective management of software licenses can help avoid purchasing too many licenses that result in unused software. In May 2014, GAO reported that most agencies, including SSA, lacked comprehensive software license policies. As a result, GAO made six recommendations to SSA, to include developing a comprehensive software licenses policy and inventory. SSA implemented all six recommendations.

However, SSA's IT management policies have not fully addressed the role of its CIO. Various laws and related guidance assign IT management responsibilities to CIOs in six key areas. In August 2018, GAO reported that SSA had fully addressed the role of the CIO in one of the six areas (see table). Specifically, SSA's policies fully addressed the CIO's role in the IT leadership and accountability area by requiring the CIO to report directly to the agency head, among other things.

In contrast, SSA's policies did not address or minimally addressed the IT workforce and IT strategic planning areas. For example, SSA's policies did not include requirements for the CIO to annually assess the extent to which personnel meet IT management skill requirements or to measure how well IT supports agency programs. GAO recommended that SSA address the weaknesses in the remaining five key areas. SSA agreed with GAO's recommendation and stated that the agency plans to implement the recommendation by the end of this month.

Extent to Which Social Security Administration Policies Addressed the Role of the Agency's Chief Information Officer, as of August 2018

Responsibility to be addressed in agency policies	GAO assessment
Information technology (IT) leadership and accountability	Fully
IT strategic planning	Minimally
IT workforce	Not at all
IT budgeting	Substantially
IT investment management	Partially
Information security	Substantially

Source: GAO analysis of Social Security Administration policies. | GAO-18-703T

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

I am pleased to be here to participate in your hearing on the Social Security Administration's (SSA) management of information technology (IT) and the authorities of its chief information officer (CIO). SSA is responsible for delivering services that touch the lives of almost every American, and the agency extensively relies 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 2018, the agency plans to spend approximately $1.6 billion on hardware and software, computer maintenance, and contractor support, among other things.

We have previously reported that federal IT projects have often failed, in part, due to a lack of oversight and governance.[1] Executive-level governance and oversight across the government has often been ineffective, in particular from CIOs. For example, our work has found that some CIOs do not have the authority to review and approve the entire agency IT portfolio.[2]

Given the challenges that federal agencies, including SSA, have long encountered in managing IT, in December 2014, Congress enacted federal IT acquisition reform legislation (commonly referred to as the *Federal Information Technology Acquisition Reform Act*, or FITARA).[3] This law was intended to improve agencies' acquisitions and enable Congress to hold agencies accountable for reducing duplication and achieving cost savings. Among other things, the law requires agency action to consolidate federal data centers, ensure adequate implementation of incremental development, review and approve IT acquisitions, purchase software government-wide, and enhance agency CIO authority.

[1]For example, GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[2]GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management,* GAO-11-634 (Washington, D.C.: Sept. 15, 2011).

[3]*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, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

In February 2015, we added improving the management of IT acquisitions and operations to our list of high-risk areas for the federal government.[4] In February 2017, we issued an update to our high-risk report and noted that, while progress has been made in addressing the high-risk area of IT acquisitions and operations, significant work remained to be completed.[5] To address these shortcomings, we have made numerous recommendations aimed at improving federal IT acquisitions and operations.[6]

At your request, my testimony today summarizes our previously reported findings regarding SSA's management of IT acquisitions and operations and the authorities of its CIO. In developing this testimony, we relied on reports that we previously issued between July 2011 and August 2018, which discussed various aspects of the agency's IT management. These reports, cited throughout this statement, include detailed information on the scope and methodology of our prior reviews. We also incorporated information on SSA's actions in response to recommendations we made in our previous reports.

We conducted the work upon which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[4]GAO, *High-Risk Series: An Update,* GAO-15-290 (Washington, D.C.: Feb. 11, 2015). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[5]GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others,* GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[6]For example, GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities,* GAO-18-93 (Washington, D.C.: Aug. 2, 2018); *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations,* GAO-18-264 (Washington, D.C.: May 23, 2018); *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions,* GAO-18-42 (Washington, D.C.: Jan. 10, 2018); *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017); and *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014).

Background

SSA's mission is to deliver Social Security services that meet the changing needs of the public. The Social Security Act and amendments[7] 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 2019, $892 billion in old-age and survivors insurance benefits are expected to be paid to a monthly average of approximately 54 million beneficiaries.
- *Disability Insurance* provides monthly benefits to disabled workers and their spouses and children. The agency estimates that, in fiscal year 2019, a total of approximately $149 billion in disability insurance benefits will be paid to a monthly average of about 10 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 2019, SSA estimates that nearly $59 billion in federal benefits and state supplementary payments will be made to a monthly average of approximately 8 million recipients.

SSA Relies Extensively on IT

SSA relies heavily on its IT resources to support the administration of its programs and related activities. For example, 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 Resources Strategic Plan*, its systems supported the processing of an average daily volume of about 185 million individual transactions in fiscal year 2015.[8]

SSA's Office of the Deputy Commissioner for Systems is responsible for developing, overseeing, and maintaining the agency's IT systems.

[7]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 SSA. See 42 U.S.C. §§ 401-434 and 42 U.S.C. §§ 1381-1383f.

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

Comprised of approximately 3,800 staff, the office is headed by the Deputy Commissioner, who also serves as the agency's CIO.

SSA Has a History of Unsuccessful IT Management

SSA has long been challenged in its management of IT. As a result, we have previously issued a number of reports highlighting various weaknesses in the agency's system development practices, governance, requirements management, and strategic planning, among other areas. [9] Collectively, our reports stressed the need for the agency to strengthen its IT management controls.

In 2016, we reported that SSA's acting commissioner had stated that the agency's aging IT infrastructure was not sustainable because it was increasingly difficult and expensive to maintain. Accordingly, the agency requested $132 million in its fiscal year 2019 budget 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 in the budget is its Disability Case Processing System, which has been under development since December 2010. This system is intended to replace the 52 disparate Disability Determination Services' component systems and associated processes with a modern, common case processing system.[10] According to SSA, the new system is to modernize the entire claims process, including case processing, correspondence, and workload management.

However, SSA has reported substantial difficulty in the agency's ability to carry out this initiative, citing software quality and poor system performance as issues. Consequently, in June 2016, the Office of

[9]See, for example, GAO, *Electronic Disability Claims Processing: SSA Needs to Address Risks Associated with Its Accelerated Systems Development Strategy,* GAO-04-466 (Washington, D.C.: Mar. 26, 2004); *Information Technology: SSA Has Taken Key Steps for Managing Its Investments, but Needs to Strengthen Oversight and Fully Define Policies and Procedures,* GAO-08-1020 (Washington, D.C.: Sept. 12, 2008); and *Social Security Administration: Improved Planning and Performance Measures Are Needed to Help Ensure Successful Technology Modernization,* GAO-12-495 (Washington, D.C.: Apr. 26, 2012).

[10]SSA is required to conduct periodic continuing disability reviews to ensure that only eligible people continue to receive benefits. SSA has agreements with state Disability Determination Services agencies to initially determine whether applicants are disabled.

Management and Budget (OMB) placed the initiative on its government-wide list of 10 high-priority programs requiring attention.[11]

Congress and the Administration Have Undertaken Efforts to Improve Federal IT

As previously mentioned, Congress enacted federal IT acquisition reform legislation (commonly referred to as FITARA) in December 2014. This legislation was intended to improve agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings. It includes specific requirements related to seven areas: (1) agency CIO authority enhancements, (2) federal data center consolidation initiative, (3) enhanced transparency and improved risk management, (4) portfolio review, (5) IT acquisition cadres, (6) government-wide software purchasing program, and (7) the Federal Strategic Sourcing Initiative.

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[12] The guidance identifies a number of actions that agencies are to take to establish a basic set of roles and responsibilities (referred to as the common baseline) for CIOs and other senior agency officials and, thus, to implement the authorities described in the law.

More recently, on May 15, 2018, the President signed Executive Order 13833, *Enhancing the Effectiveness of Agency Chief Information Officers*. Among other things, this executive order is intended to better position agencies to modernize their technology, execute IT programs more efficiently, and reduce cybersecurity risks.[13] The order pertains to 22 of the 24 Chief Financial Officers Act agencies; the Department of Defense and the Nuclear Regulatory Commission are exempt.

For the covered agencies, including SSA, the executive order strengthens the role of the CIO by, among other things, requiring the CIO to report directly to the agency head; to serve as the agency head's primary IT strategic advisor; and to have a significant role in all management, governance, and oversight processes related to IT. In addition, one of the cybersecurity requirements directs agencies to ensure that the CIO works closely with an integrated team of senior executives, including those with

[11]OMB, *Report to Congress: 10 High Priority Programs* (Washington, D.C.: June 9, 2016).

[12]OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

[13]Exec. Order No. 13833, *Enhancing the Effectiveness of Agency Chief Information Officers* (May 15, 2018).

expertise in IT, security, and privacy, to implement appropriate risk management measures.

In June 2018, we issued a report that examined the cybersecurity workforce of the government.[14] We noted that most of the 24 agencies we examined had developed baseline assessments to identify cybersecurity personnel within their agencies that held certifications, but the results were potentially unreliable. However, SSA's baseline was found to be reliable because it addressed all of the reportable information, such as the extent to which personnel without professional certifications were ready to obtain them or strategies for mitigating any gaps. Further, we found that most of the 24 agencies had established procedures to assign cybersecurity codes to positions, including SSA. We also have ongoing work at SSA, including reviewing its cybersecurity workforce; standardized approach to security assessment, authorization, and continuous monitoring; cybersecurity strategy; and intrusion detection and prevention capabilities.

From July 2011 through January 2018, we issued a number of reports that addressed specific weaknesses in SSA's management of IT acquisitions and operations and in the role of its CIO. These reports included 15 recommendations aimed at improving the agency's efforts with regard to data center consolidation, incremental development, IT acquisitions, and software licenses. We also made a recommendation to SSA to address weaknesses related to the role of the CIO in key management areas.

SSA Has Improved the Management of Selected Areas of IT Acquisitions and Operations, but Has Not Fully Addressed the Role of Its CIO

SSA has taken steps to improve its management of IT acquisitions and operations by addressing 14 of the 15 recommendations that we previously directed to the agency regarding data center consolidation, incremental development, IT acquisitions, and software licenses.

- **Data center consolidation**. OMB established the Federal Data Center Consolidation Initiative in February 2010 to improve the

[14]GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions,* GAO-18-466 (Washington, D.C.: June 14, 2018).

efficiency, performance, and environmental footprint of federal data center activities. The enactment of FITARA in 2014 codified and expanded the initiative. In addition, pursuant to FITARA, in August 2016, the Federal CIO issued a memorandum that announced the Data Center Optimization Initiative as a successor effort to the Federal Data Center Consolidation Initiative. Further, in August 2016, OMB released guidance which established the Data Center Optimization Initiative and included instructions on how to implement the date center consolidation and optimization provisions of FITARA. Among other things, the guidance required agencies to consolidate inefficient infrastructure, optimize existing facilities, improve their security posture, and achieve cost savings.

In addition, the guidance directed agencies to develop a data center consolidation and optimization strategic plan that defines the agency's data center strategy for fiscal years 2016, 2017, and 2018.[15] This strategy is to include, among other things, a statement from the agency CIO indicating whether the agency has complied with all data center reporting requirements in FITARA. Further, the guidance indicates that OMB is to maintain a public dashboard to display consolidation-related cost savings and optimization performance information for the agencies.

In a series of reports that we issued from July 2011 through August 2017,[16] we noted that, while data center consolidation could potentially save the federal government billions of dollars, weaknesses existed in agencies' data center consolidation plans and data center optimization efforts. Specifically with regard to SSA, in 2011, we reported that the agency had an incomplete consolidation

[15]OMB, *Data Center Optimization Initiative*, M-16-19 (Washington D.C.: Aug. 1, 2016).

[16]GAO, *Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal*, GAO-17-448 (Washington, D.C.: Aug. 15, 2017); *Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017); *Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established* [Reissued on March 4, 2016], GAO-16-323 (Washington, D.C.: Mar. 3, 2016); *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings*, GAO-14-713 (Washington, D.C.: Sept. 25, 2014); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal*, GAO-13-378 (Washington, D.C.: Apr. 23, 2013); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed*, GAO-12-742 (Washington, D.C.: July 19, 2012); and *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings*, GAO-11-565 (Washington, D.C.: July 19, 2011).

plan and inventory of IT assets. In 2016, we reported that SSA did not meet any of the seven applicable data center optimization targets, as required by OMB. In addition, in 2017, we reported that the agency had an incomplete data center optimization plan. We stressed that until SSA completed these required activities, it might not be able to consolidate data centers, as required, and realize expected savings.

We made a total of four recommendations to SSA in our 2011, 2016, and 2017 reports to help improve the agency's reporting of data center-related cost savings and to achieve data center optimization targets. As of September 2018, SSA had implemented all four recommendations. Consequently, the agency is better positioned to improve the efficiency of its data centers and achieve cost savings.

In addition, we reported in May 2018[17] that the agencies participating in the Data Center Optimization Initiative had communicated mixed progress toward achieving OMB's goals for closing data centers by September 2018.[18] With regard to SSA, we noted that the agency had not yet achieved its planned savings but that its data centers were among the most optimized that we reviewed. In particular, while SSA reported that it planned to save $1.08 million on its data center initiative from 2016 through 2018, it had not achieved any of those savings. However, the agency reported having met the goal of closing 25 percent of its tiered data centers.[19]

Further, SSA reported the most progress among the 22 applicable agencies in meeting OMB's data center optimization targets.[20]

[17]GAO, *Data Center Optimization: Continued Agency Actions Needed to Meet Goals and Address Prior Recommendations,* GAO-18-264 (Washington, D.C.: May 23, 2018).

[18]The 24 agencies that FITARA requires to participate in Federal Data Center Consolidation Initiative are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

[19]OMB guidance defines a tiered data center as one that uses each of the following: a separate physical space for IT infrastructure, an uninterruptible power supply, a dedicated cooling system or zone, and a backup power generator for a prolonged power outage. According to OMB, all other data centers are considered non-tiered.

[20]OMB's five data center optimization targets are for server utilization and automated monitoring, energy metering, power usage effectiveness, facility utilization, and virtualization.

Specifically, SSA reported that it had met four of the five targets. (One other agency reported that it had met three targets, 6 agencies reported having met either one or two targets, and 14 agencies reported meeting none of the targets). Consequently, we did not make any additional recommendations to SSA in our May 2018 report. We also have ongoing work involving SSA related to agencies' progress on closing data center and achieving optimization targets.

- **Incremental development**. OMB has emphasized the need to deliver investments in smaller parts, or increments, in order to reduce risk, deliver capabilities more quickly, and facilitate the adoption of emerging technologies. In 2010, it called for agencies' major investments to deliver functionality every 12 months and, since 2012, every 6 months. Subsequently, FITARA codified a requirement that covered agency CIOs certify that IT investments are adequately implementing incremental development, as defined in the capital planning guidance issued by OMB.[21] Further, subsequent OMB guidance on the law's implementation, issued in June 2015, directed agency CIOs to define processes and policies for their agencies to ensure that they certify that IT resources are adequately implementing incremental development.[22]

  In November 2017, we reported that 21 agencies, including SSA, needed to improve their certification of incremental development.[23] We pointed out that, as of August 2016, agencies had reported that 103 of 166 major IT software development investments (62 percent) were certified by the agency CIO for implementing adequate incremental development in fiscal year 2017, as required by FITARA.

  With regard to SSA, we noted that only 3 of the agency's 10 investments primarily in development had been certified by the agency CIO as using adequate incremental development, as required by FITARA. In addition, we noted that SSA's incremental development certification policy did not describe the CIO's role in the certification process or how CIO certification would be documented. However, accurate agency CIO certification of the use of adequate incremental development for major IT investments is critical to ensuring that

[21]40 U.S.C. § 11319(b)(1)(B)(ii).

[22]OMB, Management and Oversight of Federal Information Technology, M-15-14 (Washington, D.C.: June 10, 2015).

[23]GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017).

agencies are making the best effort possible to create IT systems that add value while reducing the risks associated with low-value and wasteful investments.

As a result of these findings, we recommended that SSA ensure that its CIO (1) reports major IT investment information related to incremental development accurately, in accordance with OMB guidance; and (2) updates the agency's policy and processes for the certification of incremental development and confirm that the policy includes a description of how the CIO certification will be documented. SSA agreed with our recommendations and implemented both of them. Thus, the agency should be better positioned to realize the benefits of incremental development practices, such as reducing investment risk, delivering capabilities more rapidly, and permitting easier adoption of emerging technologies.

- **IT acquisitions.** FITARA includes a provision to enhance covered agency CIOs' authority through, among other things, requiring agency heads to ensure that CIOs review and approve IT contracts. OMB's FITARA implementation guidance expanded upon this aspect of the legislation in a number of ways.[24] Specifically, according to the guidance, CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts,[25] and CIOs can designate other agency officials to act as their representatives.[26]

  In January 2018, we reported that most of the CIOs at 22 selected agencies,[27] including SSA, were not adequately involved in reviewing

[24]OMB, M-15-14.

[25]OMB's guidance states that CIOs should only review and approve individual IT contract actions if they are not part of an approved acquisition strategy or plan.

[26]OMB has interpreted FITARA's "governance process" provision to permit such delegation. That provision allows covered agencies to use the governance processes of the agency to approve a contract or other agreement for IT if the CIO of the agency is included as a full participant in the governance process. In addition, the guidance specifies that if the CIO designates another official, the CIO must retain accountability.

[27]The 22 agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

and approving billions of dollars of IT acquisitions.[28] In particular, we found that SSA's process to identify IT acquisitions for CIO review did not involve the acquisition office, as required by OMB. In addition, we noted that SSA had a CIO review and approval process in place that fully satisfied the requirements set forth in OMB's guidance. However, while SSA provided evidence of the CIO's review of most of the IT contracts we examined, the agency had not ensured that the CIO or a designee reviewed and approved each IT acquisition plan or strategy. Specifically, of 10 randomly selected IT contracts that we examined at SSA, 7 acquisitions associated with those contracts had been reviewed and approved, as required by OMB.

We pointed out that, until SSA ensured that its CIO or designee reviewed and approved all IT acquisitions, the agency would have limited visibility and input into its planned IT expenditures and would not be effectively positioned to benefit from the increased authority that FITARA's contract approval provision is intended to provide. Further, the agency could miss an opportunity to strengthen the CIO's authority and the oversight of IT acquisitions—thus, increasing the potential to award IT contracts that are duplicative, wasteful, or poorly conceived.

Accordingly, we made three recommendations to SSA to address these weaknesses. As of September 2018, the agency had made progress by implementing two of the recommendations: to ensure that (1) the acquisition office is involved in identifying IT acquisitions and (2) the CIO or designee reviews and approves IT acquisitions according to OMB guidance. By taking these actions, SSA should be better positioned to properly identify and provide oversight of IT acquisitions.

However, SSA has not yet implemented our third recommendation that it issue guidance to assist in the identification of IT acquisitions. SSA stated that, in September 2017, it updated its policy for acquisition plan approval to address this recommendation; however, upon review of this policy, we did not find guidance for identifying IT acquisitions. Without the proper identification of IT acquisitions, SSA's CIO cannot effectively provide oversight of these acquisitions.

- **Software licenses**. Federal agencies engage in thousands of software licensing agreements annually. The objective of software

[28]GAO, *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions,* GAO-18-42 (Washington, D.C.: Jan. 10, 2018).

license management is to manage, control, and protect an organization's software assets. Effective management of these licenses can help avoid purchasing too many licenses, which can result in unused software, as well as too few licenses, which can result in noncompliance with license terms and cause the imposition of additional fees.

As part of its PortfolioStat initiative, OMB has developed policy that addresses software licenses.[29] This policy requires agencies to conduct an annual, agency-wide IT portfolio review to, among other things, reduce commodity IT spending. Such areas of spending could include software licenses.

In May 2014, we reported on federal agencies' management of software licenses and determined that better management was needed to achieve significant savings government-wide.[30] Of the 24 agencies we reviewed, SSA was 1 of 22 that lacked comprehensive policies that incorporated leading practices.[31]

In particular, SSA's policy partially met four of the leading practices and did not meet one. Further, we noted that SSA was among 22 of the 24 selected agencies that had not established comprehensive software license inventories—a leading practice that would help the agencies to adequately manage their software licenses.

As such, we made six recommendations to SSA to improve its policies and practices for managing software licenses. These included recommendations that the agency develop a comprehensive policy for the management of software licenses and establish a comprehensive inventory of software licenses. SSA agreed with the recommendations and, as of September 2018, had implemented all six of them. As a result, the agency should be better positioned to manage its software licenses and identify opportunities for reducing software license costs.

[29]PortfolioStat is an OMB initiative which requires agencies to conduct annual reviews of their IT investments and make decisions on eliminating duplication, among other things.

[30]GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014).

[31]The five leading practices we identified in our May 2014 report are: centralizing management; establishing a comprehensive inventory of licenses; regularly tracking and maintaining comprehensive inventories using automated tools and metrics; analyzing the software license data to inform investment decisions and identify opportunities to reduce costs; and providing appropriate personnel with sufficient training on software license management.

SSA Needs to Further Address the CIO's Role in Its Policies

While SSA has taken steps that improved its IT management in the areas of data center consolidation, incremental development, IT acquisitions, and software licenses, we reported in August 2018 that the agency had not fully addressed the role of the CIO in its policies.[32]

As previously mentioned, FITARA and the President Executive Order 13833, among other laws and guidance, outline the roles and responsibilities for agency CIOs in an attempt to improve the government's performance in IT and related information management functions. Within these laws and guidance, we identified IT management responsibilities assigned to CIOs in six key IT areas:[33]

- **Leadership and accountability.** CIOs are responsible and accountable for the effective implementation of IT management responsibilities. For example, CIOs are to report directly to the agency head or that official's deputy and designate a senior agency information security officer.
- **Strategic planning.** CIOs are required to lead the strategic planning for all IT management functions. An example of a CIO requirement related to the strategic planning area is measuring how well IT supports agency programs and reporting annually on the progress in achieving the goals.
- **IT workforce.** CIOs are to assess agency IT workforce needs and develop strategies and plans for meeting those needs. For example, CIOs are responsible for annually assessing the extent to which agency personnel meet IT management knowledge and skill requirements, developing strategies to address deficiencies, and reporting to the head of the agency on the progress made in improving these capabilities.
- **IT budgeting.** CIOs are responsible for the processes for all annual and multi-year IT planning, programming, and budgeting decisions. For example, CIOs are to have a significant role in IT planning, programming, and budgeting decisions.
- **IT investment management.** CIOs are to manage, evaluate, and assess how well the agency is managing its IT resources. In

[32]GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

[33]These laws include FITARA, FISMA (44 U.S.C. § 3554 et al.), the Paperwork Reduction Act (44 U.S.C. § 3506 et al.), and the Clinger-Cohen Act (40 U.S.C. §§ 11312 and 11313).

particular, CIOs are required to improve the management of the agency's IT through portfolio review.

- **Information security.** CIOs are to establish, implement, and ensure compliance with an agency-wide information security program. For example, CIOs are required to develop and maintain an agency-wide security program, policies, procedures, and control techniques.

In our August 2018 report, we noted that SSA, along with 23 other agencies, did not have policies that fully addressed the role of the CIO in these six key areas, consistent with the laws and guidance.

To its credit, SSA had fully addressed the role of the CIO in the IT leadership and accountability area. In particular, the agency's policies addressed the requirements that the CIO report directly to the agency head, assume responsibility and accountability for IT investments, and designate a senior agency information security officer.

However, the policies did not fully address the role of the CIO in the other five areas (i.e., strategic planning, workforce, budgeting, investment management, and information security). For example, the agency's policies did not address the IT workforce area at all, including the requirements that the CIO annually assess the extent to which agency personnel meet IT management knowledge and skill requirements, develop strategies to address deficiencies, and report to the head of the agency on the progress made in improving these capabilities.

Further, SSA's policies minimally addressed the requirements for IT strategic planning. Specifically, while the agency's policies required the CIO to establish goals for improving agency operations through IT, the policies did not require the CIO to measure how well IT supports agency programs and report annually on the progress in achieving the goals.

Table 1 summarizes the extent to which SSA's policies addressed the role of its CIO, as reflected in our August 2018 report.

Table 1: Extent to Which Social Security Administration Policies Addressed the Role of Its Chief Information Officer, as of August 2018

Responsibility to be addressed in agency policies	GAO assessment
Information technology (IT) leadership and accountability	Fully
IT strategic planning	Minimally
IT workforce	Not at all
IT budgeting	Substantially
IT investment management	Partially
Information security	Substantially

Source: GAO analysis of Social Security Administration policies. | GAO-18-703T

Key:

Fully – the agency provided evidence that described the CIO's role for carrying out all of the related responsibilities

Substantially - the agency provided evidence that described the CIO's role for at least two-thirds, but not all, of the related responsibilities

Partially - the agency provided evidence that described the CIO's role for at least one-third, but less than two-thirds, of the related responsibilities

Minimally - the agency provided evidence that described the CIO's role for less than one-third of the related responsibilities

Not at all - the agency did not provide evidence that described the CIO's role for carrying out the any of the related responsibilities

As a result of these findings, we made a recommendation to SSA to address the weaknesses in its policies with regard to the remaining five key management areas. In response, the agency agreed with our recommendation and, subsequently, stated that it planned to do so by the end of September 2018. Following through to ensure that the identified weaknesses are addressed in its policies will be essential to helping SSA overcome its longstanding IT management challenges.

In conclusion, effective IT management is critical to the performance of SSA's mission. Toward this end, the agency has taken steps to improve its management of IT acquisitions and operations by implementing 14 of the 15 recommendations we made from 2011 through 2018 to improve its IT management. Nevertheless, SSA would be better positioned to effectively address longstanding IT management challenges by ensuring that it has policies in place that fully address the role and responsibilities of its CIO in the five key management areas, as we previously recommended.

Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staffs have any questions about this testimony, please contact Carol C. Harris at (202) 512-4456 or harriscc@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 Kevin Walsh (Assistant Director), Jessica Waselkow (Analyst in Charge), and Rebecca Eyler.