

**THE STATE OF SOCIAL SECURITY'S
INFORMATION TECHNOLOGY**

HEARING
BEFORE THE
SUBCOMMITTEE ON SOCIAL SECURITY
OF THE
COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 27, 2018

Serial No. 115-SS12

Printed for the use of the Committee on Ways and Means



U.S. GOVERNMENT PUBLISHING OFFICE

33-875

WASHINGTON : 2019

COMMITTEE ON WAYS AND MEANS

KEVIN BRADY, Texas, *Chairman*

SAM JOHNSON, Texas
DEVIN NUNES, California
DAVID G. REICHERT, Washington
PETER J. ROSKAM, Illinois
VERN BUCHANAN, Florida
ADRIAN SMITH, Nebraska
LYNN JENKINS, Kansas
ERIK PAULSEN, Minnesota
KENNY MARCHANT, Texas
DIANE BLACK, Tennessee
TOM REED, New York
MIKE KELLY, Pennsylvania
JIM RENACCI, Ohio
KRISTI NOEM, South Dakota
GEORGE HOLDING, North Carolina
JASON SMITH, Missouri
TOM RICE, South Carolina
DAVID SCHWEIKERT, Arizona
JACKIE WALORSKI, Indiana
CARLOS CURBELO, Florida
MIKE BISHOP, Michigan
DARIN LAHOOD, Illinois
BRAD R. WENSTRUP, Ohio

RICHARD E. NEAL, Massachusetts
SANDER M. LEVIN, Michigan
JOHN LEWIS, Georgia
LLOYD DOGGETT, Texas
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR., New Jersey
JOSEPH CROWLEY, New York
DANNY DAVIS, Illinois
LINDA SANCHEZ, California
BRIAN HIGGINS, New York
TERRI SEWELL, Alabama
SUZAN DELBENE, Washington
JUDY CHU, California

GARY J. ANDRES, *Staff Director*

BRANDON CASEY, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

MIKE BISHOP, Michigan
VERN BUCHANAN, Florida
MIKE KELLY, Pennsylvania
TOM RICE, South Carolina
DAVID SCHWEIKERT, Arizona
DARIN LAHOOD, Illinois

JOHN B. LARSON, Connecticut
BILL PASCRELL, JR., New Jersey
JOSEPH CROWLEY, New York
LINDA SANCHEZ, California

CONTENTS

	Page
Advisory of September 27, 2018, announcing the hearing	2
WITNESSES	
Rajive Mathur, Chief Information Officer and Deputy Commissioner for Systems, Social Security Administration	6
Gale Stallworth Stone, Acting Inspector General, Social Security Administration	18
Carol C. Harris, Director, Information Technology Management Issues, Government Accountability Office	27
QUESTIONS FOR THE RECORD	
Questions from Social Security Subcommittee Chairman Sam Johnson to Carol C. Harris, Director, Information Technology Management Issues, Government Accountability Office	65
Questions from Social Security Subcommittee Chairman Sam Johnson to Rajive Mathur, Chief Information Officer and Deputy Commissioner for Systems, Social Security Administration	70
Question from Representative Mike Bishop to Rajive Mathur, Chief Information Officer and Deputy Commissioner for Systems, Social Security Administration	71
Questions from Representative Carlos Curbelo to Rajive Mathur, Chief Information Officer and Deputy Commissioner for Systems, Social Security Administration	71
Questions from Social Security Subcommittee Chairman Sam Johnson to Gale Stallworth Stone, Acting Inspector General, Social Security Administration	76
SUBMISSIONS FOR THE RECORD	
Domtar	78
Jacqueline Marie Merson, Attorney at Law	80
Consumer First Coalition (CFC)	81

**THE STATE OF SOCIAL SECURITY'S
INFORMATION TECHNOLOGY**

THURSDAY, SEPTEMBER 27, 2018

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 11:01 a.m., in Room 2020, Rayburn House Office Building, Hon. Sam Johnson [Chairman of the Subcommittee] presiding.
[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
Thursday, September 27, 2018
SS-12

CONTACT: (202) 225-3625

Chairman Johnson Announces Hearing on the State of Social Security's Information Technology

House Ways and Means Social Security Subcommittee Chairman Sam Johnson (R-TX), announced today that the Subcommittee will hold a hearing entitled "The State of Social Security's Information Technology." The hearing will focus on the Social Security Administration's information technology, including modernization, management, and acquisitions. **The hearing will take place on Thursday, September 27, 2018, in room 2020 of the Rayburn House Office Building, beginning at 11:00 a.m.**

In view of the limited time to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit written comments for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, <http://waysandmeans.house.gov>, select "Hearings." Select the hearing for which you would like to make a submission, and click on the link entitled, "[Click here to provide a submission for the record.](#)" Once you have followed the on-line instructions, submit all requested information. ATTACH your submission as a Word document, in compliance with the formatting requirements listed below, **by the close of business on Thursday, October 11, 2018.** For questions, or if you encounter technical problems, please call (202) 225-3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

All submissions and supplementary materials must be submitted in a single document via email, provided in Word format and must not exceed a total of 10 pages. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. The name, company, address, telephone, and fax numbers of each witness must be included in the body of the email. Please exclude any personal identifiable information in the attached submission.

Failure to follow the formatting requirements may result in the exclusion of a submission. All submissions for the record are final.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-225-1721 or 202-226-3411 TDD/TTY in advance of the event (four business days' notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available at <http://www.waysandmeans.house.gov/>

Chairman JOHNSON. Good morning. Welcome to today's hearing on the state of Social Security's information technology.

Before we dive into this important subject, I would like to take a few words of thanks since this is the last hearing I plan to hold as the Subcommittee Chairman.

As Chairman, I have focused on many challenges facing Social Security, including the need to modernize the disability program; combat fraud; protect Americans from identity theft; and make sure our children and grandchildren can count on Social Security, just like seniors and individuals with disabilities do today.

And I thank my colleagues on the Social Security Subcommittee for the honor of serving with them on behalf of the American people.

I also want to thank the Subcommittee staff who work behind the scenes to help make our successes possible. In particular, I want to recognize Amy Shuart, Kim Hildred, and Ted McCann, as well as Kathryn Olson. Some are behind us, by the way.

I am proud to say that one of this Subcommittee's recent successes is the bipartisan Representative Payee bill that became law earlier this year.

John, we did this together, and I want to give you a copy of the bill. You have been a good friend, and it has been a pleasure to lead this Subcommittee with you. God bless you. I appreciate you, partner.

Mr. LARSON. You too, partner.

Chairman JOHNSON. Where is the bill? There it is. And I wrote a note on it. God bless you.

[Laughter.]

Mr. LARSON. Thank you, Mr. Chairman. I especially appreciate the handwritten note at the bottom. God bless you.

Chairman JOHNSON. God bless you, sir. It has been a pleasure working with you.

Mr. LARSON. An honor to work with you.

Thank you, sir.

Chairman JOHNSON. Now, back to the issue at hand: Social Security's information technology.

While Social Security faces many challenges, information technology is among the most critical to providing the exceptional service Americans expect and deserve. That is why, over the years, the Subcommittee has continued to focus on this important topic. In fact, the first hearing that I ever held as Chairman back in 2011 was on replacing Social Security's aging data center.

Although Social Security now has modern hardware and modern data centers, its employees are still using software that is decades out of date. And about 30 percent of these legacy systems still use

COBOL codes, an ancient programming language that isn't even taught in schools anymore.

Maintaining systems that old isn't easy. These outdated systems require extra training for employees. And these systems also make it hard for Social Security to respond, as needed, to changes, not to mention the simple fact that it is expensive to maintain old, custom-built systems.

But I also have some good news to share. After releasing a modernization plan last October, Social Security has started to make some real progress in bringing the agency's information technology into the 21st century. Social Security is undergoing a technology transformation that is long overdue.

These changes will not only make sure Social Security can quickly respond to new challenges, but also that the agency is serving Americans in a modern way. Social Security is finally on the way to getting rid of outdated green-screen technology.

But there is still a long way to go. It is going to take consistent leadership at Social Security, and it is going to take continued oversight from Congress to make sure Social Security isn't just spinning its wheels.

Social Security must learn from the mistakes of DCPS and other smaller projects, like "Click to Chat." This latter project ended up costing more than double what Social Security's original expectation was. Taxpayers cannot afford IT projects that unnecessarily drag on for years or that double in cost. Social Security must find a way to better use private-sector alternatives to keep costs down and projects on schedule.

Having a modern IT infrastructure is going to be critical for Social Security's future, and I look forward to hearing how Social Security can get there on time and on budget. Americans want, need, and deserve nothing less.

I thank our witnesses for being here today, and I look forward to hearing their testimony. I now recognize Mr. Larson for his opening statement.

Mr. LARSON. Thank you, Mr. Chairman. And it is with no small amount of sentiment that we gather today. And what a great honor it is to serve with you in the United States Congress, and even more of an honor to have been the Ranking Member and to have been able to work with you in a collaborative nature.

In a time when solutions oftentimes elude the United States Congress, to work with somebody who has always put America first, who has always looked at the Social Security issues in a non-partisan way, in a way in which—all he has ever done throughout his life is to try to make the country a little safer and a little better.

As a freshman Member of Congress, one of the first bills I was able to get passed was a bill that created a history of the House of Representatives. Robert Remini, the historic figure, University of Chicago, authored that book. It is hard to imagine that one could sit in Congress on a committee and serve with Sam Johnson and John Lewis. But that is the nature of the Ways and Means Committee.

And if you are not humbled by their service prior to ever coming to Congress, then you don't know much about American history or

about the sacrifice and the character of this remarkable man. To watch him work with the staffs collectively, work well, and always do it in the fairest and the most considerate and—as I think everybody acknowledges—one of the grand gentlemen of the United States Congress.

So to—as he pointed out, you know, to work on the payee bill together, but to work on so many other small initiatives. And just the cordiality and the camaraderie and the roll-up-your-sleeves and get-the-job-done attitude that he brings to Congress every day is pretty remarkable.

It was also my great honor to create a medal in the United States Congress that is named after Sam Johnson and John Lewis for their incredible patriotism. Would it be there was more of that in Congress today, and more getting after solutions. But I can say this without hesitation: That has always been his goal, as the Chairman of this Committee.

I so appreciate everything that he has been doing and, as he indicated, getting after fraud, getting after—working on behalf, especially, of children and families and disability issues that he knows better than most, because he has lived them.

What an honor to serve with him, to serve alongside of him. And it is just—as I tell my children, it is just my hope that some of his true, genuine Americanism rubs off and helps you become a better person, having known and served with him.

With that, we are excited to hear from our witnesses this afternoon. And, again, the Chairman has indicated the need for modernization and everything that we need to look at, you know, to combat synthetic identity theft to making sure the delivery system that we have at Social Security, and especially the continuity that we know is so vitally important to the citizens we are sworn to serve, remains in place.

I look forward to the hearing. And, again, Mr. Chairman, a tremendous debt of gratitude to be afforded the honor of serving with you.

Chairman JOHNSON. Thank you, sir. I appreciate those comments. God bless you.

As is customary, any Member is welcome to submit a statement for the hearing record.

Before we move to our testimony today I want to remind our witnesses to please limit your oral statements to 5 minutes. However, without objection, all of the written testimony will be made a part of the hearing record.

We have three witnesses today. Seated at the table are Rajive Mathur, Chief Information Officer and Deputy Commissioner for Systems of the Social Security Administration; Gale Stallworth Stone, Acting Inspector General of the Social Security Administration; and Carol Harris, Director, Information Technology Management Issues, Government Accountability Office.

I thank you all for being here today.

Mr. Mathur, welcome. Again, thanks for being here. And please proceed.

STATEMENT OF RAJIVE MATHUR, CHIEF INFORMATION OFFICER AND DEPUTY COMMISSIONER FOR SYSTEMS, SOCIAL SECURITY ADMINISTRATION

Mr. MATHUR. Thank you, Mr. Chairman. Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, thank you for the opportunity to discuss Social Security's information technology.

I am Rajive Mathur, Social Security's Chief Information Officer and Deputy Commissioner for Systems. Prior to joining the SSA in 2017, I worked in leadership roles in both the private and public sectors.

Social Security touches the lives of nearly every person in America, whether at the birth of a child, after the loss of a loved one, at the onset of disability, or at the transition of work to retirement. In fiscal year 2018 we expect to pay over \$1 trillion in benefits to an average of over 70 million monthly beneficiaries.

Information technology is vital to nearly every aspect of the work we do to serve the public, from taking claims to protecting the sensitive personal information we maintain, to preventing fraud and improper payments in our programs across government. Most of our core systems are over 30 years old. Over the years we have expanded their capabilities to keep up with the changes in our programs and business processes. However, much of the underlying design was set when they were first built.

For example, our core systems rely on COBOL, which is a programming language from the 1950s. While these systems have performed admirably and have allowed us to provide uninterrupted service for many years, their underlying design limits what we can accomplish and our ability to adapt to change. It also makes the systems expensive to maintain and, as more of our IT workforce approaches retirement, we risk losing the institutional knowledge needed to maintain them.

Accordingly, we have begun a 5-year plan to modernize our software, our hardware, and our infrastructure, using modern code and architecture. And as we close our first year executing our IT modernization plan, I am happy to report that we are on schedule and on budget.

Some of our accomplishments this year include eliminating the remaining green screens that our employees use to take SSI claims and replacing them with web-based interfaces, and converting our remaining master file to an industry standard format. Looking ahead, I am excited by what IT modernization has in store.

In mid-fiscal year 2019 we will release the product that is the first release of software to provide front-line employees with a person-centric view of the individual that they are serving, including the person's visits, the notices that they have received, and actions that may be pending in their case. This will eliminate the need for employees to access various systems for the information they need to provide great service, and it is one of the most commonly requested enhancements.

In addition to modernizing systems, we also have been modernizing the structure of our organization, our IT organization, and the methods that we use to manage and develop IT. By strengthening internal collaboration and using Agile methodologies, we have fo-

cused on delivering software capabilities early, and continuously enhancing them based on direct feedback from the users.

For example, we have been using Agile to develop DCPS2, which is a national, common-case processing system for State DDSs. We have regularly added functionality to DCPS2 as we have expanded it to 10 States, with 4 more joining soon, and 34 others that are scheduled for deployment.

We are delivering products on time. Our systems are available to users 99.96 percent of the time. And we have reduced the number of IT outages.

As Chief Information Officer, one of my goals has been to build a modern IT organization for the next generation, one that is accountable, competent, transparent, and secure, one that is focused on understanding and meeting the needs of the public and our employees.

We have a large IT enterprise and are working quickly to make big changes, even while we work to maintain the security and availability of our systems, and we continue to deploy needed software that, while it is not part of the modernization program, is still built on modern technology.

IT modernization is a significant investment. We will invest \$691 million over the next 5 years, including the \$280 million that Congress appropriated in fiscal year 2018.

We appreciate Congress'—and particularly this Subcommittee's—support.

I also want to take this opportunity to recognize Chairman Johnson.

Mr. Chairman, you have long understood the direct connection between SSA's IT and its ability to serve the people who count on its programs. Thank you for your leadership on this issue, and for being a champion of the Social Security program.

On behalf of all of us at SSA, please accept my best wishes for your retirement.

Thank you for the opportunity to appear before you today, and I would be happy to answer any questions.

[The prepared statement of Mr. Mathur follows:]



**COMMITTEE ON WAY AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES**

SEPTEMBER 27, 2018

STATEMENT FOR THE RECORD

**RAJIVE MATHUR
CHIEF INFORMATION OFFICER &
DEPUTY COMMISSIONER FOR SYSTEMS
SOCIAL SECURITY ADMINISTRATION**

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

Thank you for inviting me to discuss modernizing information technology (IT) at the Social Security Administration (SSA). I am Rajive Mathur, SSA's Chief Information Officer (CIO) and Deputy Commissioner for Systems.

Before beginning my testimony, I want to first take the opportunity to recognize Chairman Johnson for his leadership on this issue. For many years, you have stressed the importance of modernizing our information technology. Now, because of your and the Congress's support, we are engaged in that effort. Our IT modernization program will have a tangible effect on the lives of those who are counting on Social Security. As you look back on your long career of public service accomplishments, I hope you count this achievement among your proudest. On behalf of all of us at the Social Security Administration, please let me congratulate you and wish you and your family the best in retirement.

Our Programs and Organization

Social Security touches the lives of nearly every American, whether at the birth of a child, the loss of a loved one, the onset of a disability, or the transition from work to retirement. For more than 80 years, our programs have provided a safety net for the public and have contributed to the financial security of the elderly and the disabled. In Fiscal Year (FY) 2018, we expect to pay over \$1 trillion in benefits to Social Security beneficiaries and Supplemental Security Income (SSI) recipients. Each month, we pay, on average, more than 70 million Social Security beneficiaries and SSI recipients.

Our approximately 63,000 Federal employees and 15,000 State employees serve the public through a network of more than 1,200 field offices, a national toll-free number, eight processing centers, 52 State agencies that make disability determinations, and more than 160 hearing offices. Every day, about 170,000 people visit and 250,000 people call one of our field offices. This FY, we expect to:

- handle approximately 33 million calls on our National 800 Number;
- complete over 5.8 million claims for retirement and survivor benefits, 2.3 million initial disability claims, 518,000 reconsiderations, and 759,000 hearing dispositions;
- complete about 17 million original and replacement Social Security card applications; and
- complete 890,000 full medical Continuing Disability Reviews and nearly 2.9 million SSI non-medical redeterminations.

We offer highly-rated online services for those who choose to do business with us online, and in FY 2017, the public completed 155 million transactions using our website.

In addition to our direct service to the public, we perform critical work that supports the efficiency and effectiveness of programs across the government. We process all employer wage reports (forms W-2) as an agent of the Internal Revenue Service (IRS), from which we obtain the earnings

information we need to accurately calculate Social Security benefits, and information the IRS needs for tax administration. Last year we posted over 279 million earnings items to workers' records.

In addition, when authorized by law, we share the data we maintain on beneficiaries and individuals with other Federal and State agencies, who use it to prevent improper payments, collect taxes, provide health insurance, and more. We have thousands of such data exchanges. In FY 2017, we performed more than 2.1 billion automated Social Security number verifications that, among other things, allow employers to more accurately report wages to us.

Information Technology at SSA

The scope of our programs is immense, and information technology is vital to nearly every aspect of the work we do to serve the public. IT allows our field office employees to collect pertinent information and perform complex benefit calculations; it provides for electronic storage and retrieval of medical records and other information; it protects the sensitive personal, benefits, and earnings information that we maintain; and it helps identify and prevent fraud and improper payments in our programs and across government.

Our IT program operates in a bi-modal environment. That is, we concurrently develop new IT capabilities, while providing stable access to our existing systems. We are continuously engaged in activities related to IT planning, building new capabilities or purchasing them from the private sector, and operating and protecting our current systems.¹ I like to describe it as reengineering the plane while it's in the air. Since becoming CIO, one of my focuses has been to ensure that we have sound governance and processes in place for each of these categories of activities, and that we are identifying and capturing metrics in each area so we can evaluate our performance.

Most of our core systems are over 30 years old. Over the years, we have modified and expanded their capabilities to keep up with changes in the law and in our regulations, policies, and business processes. However, much of their underlying design was established when these systems were first built decades ago. For example, our core systems still rely on COBOL, a programming language that was created in the 1950s.

While these systems have performed capably—allowing us to provide uninterrupted services for many years—this old foundation limits what we can accomplish and our ability to adapt to changes, and has forced us to deliver IT functionality that gets the job done but does not keep up with either the public's or our own employees' expectations. It also makes our IT more expensive to maintain. Our total IT expenditures in FY 2017, including our staff and contractors, was about \$1.8 billion, or about 14.6 percent of our total expenses, and the majority of that was used for the ongoing costs of maintaining our existing applications

Many experienced employees in our IT workforce are approaching retirement age, especially those employees who are experts in handling COBOL. We will be losing the expertise of our existing systems that they have built up over time. Our newer employees are highly skilled and capable of maintaining our level of service, but many have not developed the in-depth knowledge of our

¹ See Appendix A for an illustration of these activities.

existing systems that is necessary to add incremental improvements or help us recover if a significant software issue were to arise.

Modernizing our Information Technology

We have embarked on modernizing our entire IT program. Our five-year plan will modernize Social Security's major systems using modern architectures; product investment techniques, such as agile software engineering methods; cloud provisioning; and shared services.² The goals of our IT Modernization Plan are:

- **Improve Service to the Public** through increasing online services, real-time processing, and having a more service-centric organization, technical structure, and overall better customer experience.
- **Increase the Value of IT for Business** by increasing IT and data reliability, security, and enabling faster claim and post-entitlement decisions.
- **Improve IT Workforce Engagement** by enabling a quicker path to fielding new capabilities, modernizing the development environment to improve productivity, and building a culture to attract new and retain our current top technology talent.
- **Improve Business Workforce Engagement** by enabling better service with enhanced user-centric tools and the ability to move routine work through the systems quickly, enabling our workforce to focus more on the most challenging service needs.
- **Reduce IT and other Operating Costs** through expanding shared services, the cloud, and Commercial Off-The-Shelf (COTS) packages, increasing benefits available through disciplined approaches and reuse of code, and encouraging innovation to improve operational efficiency.
- **Reduce Risk to Continuity of Operations** by increasing awareness of cyber threats and capacity to defend against these threats, and by replacing time-worn systems with maintainable technology.

This initiative will transform all dimensions of SSA's IT program, from our software, to our hardware and infrastructure, to the structure of our IT organization itself and the processes we use to procure and develop IT products. We will build a modern IT organization that is fast, accountable, competent, transparent, secure, and laser focused on understanding and meeting the needs of the public and our employees. It will involve not only modernizing our IT program, but also reengineering our business processes to improve the effectiveness and efficiency of our programs.

Our modernized systems will streamline processes in a user-friendly and intuitive way for our front-line employees. Automation will relieve employees of having to perform many of the routine tasks that today require manual entry and re-entry, which will reduce errors. Our employees will have a complete view of a person's interactions with SSA, which will facilitate better and more consistent service. The system will facilitate completing transactions at the first point of contact by replacing overnight processing of transactions with real-time processing where possible. If real-time

² My testimony summarizes our IT Modernization Plan. Our full plan is available on our website at <https://www.ssa.gov/agency/materials/IT-Mod-Plan.pdf>

processing is not feasible, we will put in place better tools to test whether all the necessary information has been provided. Doing so will reduce the need to re-contact an individual for additional information and reduce the amount of manual rework, thus providing more efficient and responsive service to the public, while reducing administrative costs.

Our modernized systems will be less expensive to maintain and easier to update. IT modernization will put SSA in a better position to respond more quickly and less expensively to program changes and the evolving expectations of our employees and the American public. We will also be better able to integrate future technological advancements and data sharing with other agencies.

Modernizing Core Programmatic Business Processes

Our modernization plan addresses the redesign of core programmatic business processes, the technology that underlies them, and the methods we use to develop them. The programmatic systems work under IT Modernization is divided into six major business areas, or “domains.” Each domain has specific objectives and outcomes, as well as dedicated IT and business staff to plan and complete the work. Below is an overview of these programmatic domains:

- **Communications** –We engage with the public through face-to-face field office visits, call centers, and by mail. This domain focuses on developing a comprehensive approach to how we connect with the public, which includes developing additional communications channels, updating communications systems and infrastructure, and ensuring that are communications are clear and concise.
- **Disability** – Our existing disability systems are a collection of several, inter-related subsystems, each designed to facilitate a part of the disability determination process, from intake (in a field office or via the phone or internet) through hearings and appeals. This domain focuses on streamlining workflow and leveraging modern technology to support the full life cycle of a disability claim, in order to expedite and simplify processing, and improve service.
- **Title II** – We have already made strides in modernizing our Title II system, which supports our Old Age, Survivors and Disability Insurance (OASDI) programs (commonly referred to as “Social Security”). This domain focuses on reducing operational and maintenance costs; providing additional safe, secure, and convenient online services; increasing automation; and reducing situations that require us to re-contact an applicant to obtain additional information.
- **Title XVI** – In recent years, we have also made strides in modernizing our Title XVI system—which supports the SSI program, our means tested program for people who are blind, disabled, or aged 65 or older—by converting its database to a modern structure and replacing green screens with web-based interfaces. This domain focuses on building on that progress by automating more actions and adding more tools to reduce improper payments.
- **Earnings** – This domain focuses on more quickly processing the millions of wage reports we receive each year and providing additional tools for employers to report and correct those reports. We will take advantage of new technologies to reduce maintenance costs, increase flexibility, and accelerate our development and deployment process.

- **Enumeration** – This domain focuses on improving the methods our employees use to access, and the infrastructure behind, the “Numident,” which is our database of records concerning the Social Security numbers we have assigned. We will modernize user interfaces, update and automate business processes, and replace out-of-date technologies with a more robust infrastructure.

Modernizing Our Infrastructure

Our modernization plan also includes three technical domains to facilitate the programmatic systems changes I described above and allow us to maintain expected levels of service. Below is an overview of these technical domains:

- **Infrastructure** – This domain focuses on modernizing the underlying technology and processes that enable the programmatic changes I described above. This includes modernizing the methods we use to develop IT products; using cloud technologies to improve availability, flexibility and cost effectiveness; and providing multiple alternative computing platforms for each modernized system to enable the optimal platform for each situation.
- **Data** – This domain focuses on consolidating our data, using state-of-the-art approaches to simplify, organize and provide data and services to fully modernized systems, which can more effectively use data. Retiring legacy data sources and formats in favor of modern tools and techniques will optimize the way we store and process data, and improve data quality. Moreover, it will provide an integrated source of historical data for business intelligence and predictive analytics across the agency.
- **Cybersecurity** – Cybersecurity is a top priority, and securing the systems and data we need to administer our programs is foundational to our modernization efforts. This domain is focused on addressing ongoing cyber threats and ensuring that data and business processes remain safe and secure. It involves incorporating security and privacy controls into our applications and the design of our IT environments and systems. It also involves adding security controls to address the risks inherent in our legacy applications, ensuring employees have access to resources appropriate for their role and job function, continuous monitoring, and a comprehensive integrity review process.

Focusing on Success

To achieve our IT modernization goals, we will invest \$691 million over five years, including the \$280 million that Congress appropriated in FY 2018. This dedicated funding has allowed us to increase the quality and accelerate the pace of delivering public-facing services.

This is a considerable investment, and successfully delivering on our plan is a top priority. Active and engaged leadership is critical for success, as any endeavor of this magnitude carries significant risks. In 2016, we established the Information Technology Investment Review Board (ITIRB), which governs SSA’S IT investment executive decision making and oversight process. As CIO, I chair the ITIRB, with the rest of the board consisting of the top executives for SSA components. Through the ITIRB, we ensure that investment proposals undergo rigorous planning, informed investment selection, transparent investment control, and relevant investment evaluation to provide

the greatest benefit to SSA's mission and to the taxpayer. For all investment proposals, the ITIRB process requires us to consider whether we can purchase COTS software or whether an internal build is required. It is important to note that when commercial software is available, in most cases we still need to do development work to integrate such software into our systems.

In addition to governing our regular IT investment decision making process, the ITIRB is engaged and focused on IT modernization. Furthermore, we have established a Program Management Office (PMO), led by a Chief Program Officer (CPO), with end-to-end accountability and associated decisional authority for delivering IT modernization. The CPO has built a PMO team with key resources from our systems and business components to oversee the functions required to execute the plan. The intent is to make sure the decisions and direction of the IT Modernization effort, along with potential impacts on other programmatic areas, are well coordinated and communicated throughout execution.

We have not only strengthened leadership and management oversight, but also changed the day-to-day processes by which we develop IT products. We have adopted a product investment approach, which places a premium on understanding the needs of customers (i.e. the public or our employees) and cross-component collaboration. Our product management teams continuously work to understand the customers, to successfully develop the IT products that meet their needs.

This approach includes transitioning away from using primarily the older, waterfall model to develop IT products. The waterfall method requires stakeholders to specify the software's requirements up front before moving to software development, and traditionally involves less direct involvement between the customers and developers.

We are moving to a modern Agile IT development model. The Agile method consists of using iterative cycles of design and development to incrementally develop software components using small, self-managed teams comprising subject matter experts from across organizational component lines. The key feature of the Agile method is its focus on meeting the unique and constantly evolving requirements and expectations of the end user, using short time frames (or "sprints") to develop software that is immediately shared with users for feedback.

We have successfully used Agile methods to develop products such as IMAGEN, which extracts information from medical evidence, and Insight, a decisional quality tool. In addition, we are using Agile methods to modernize a national system for disability case processing. This modern system will allow for the replacement of outdated, independently-operated legacy systems used by State agencies (the Disability Determination Services (DDS)) with a common, national disability case processing system (DCPS2). This modern, national system will simplify system support and maintenance, improve speed and quality of the disability determination process, and reduce administrative costs. In addition, it provides efficiency, consistency, and flexibility as we will be able to nationally implement software enhancements and modifications, including as required by evolving laws, regulations, and policy.

Currently, ten DDSs are using DCPS2 in production environments, and we will continue product development and rollout to additional DDSs in FYs 2019 and 2020. This year, we focused on increasing functionality, enabling users to process additional categories of disability claims. In

January 2018, DCPS2 delivered core case processing functionality on schedule. Core functionality included adult and child case processing for both initial and reconsideration cases. Throughout FY 2018, we steadily have increased functionality, working closely with users to assess and prioritize release of bimonthly product increments.

Our Progress and Accomplishments

I am proud of the progress we have made in concurrently implementing our IT modernization plan and deploying new applications and enhancements, while maintaining the security and availability of our systems. I am happy to report that our IT modernization effort is on schedule and on budget. In addition, I want to share with you some examples of our other, recent IT accomplishments:

Programmatic Applications

- **SSI Modernization (February, May)** – We eliminated green screens that employees use to document SSI claims information, and replaced them with modern web screens. This also eliminated the COBOL code supporting those screens.
- **Hearings and Appeals Case Management System (June)** – We released the Case Analysis Tool to assist in the development, writing, and decision-making for hearing cases.
- **Insight (March, June, and August)** – Initially developed for use in the Office of Appellate Operations, we subsequently deployed this decisional quality tool to all hearings offices.
- **IMAGEN (August)** – We began testing an application that uses natural language processing and related technologies to extract relevant content from medical evidence of record (MER), which makes it easier for disability adjudicators to search, filter, and identify the necessary content for adjudicating disability claims.

Customer Service Tools

- **Click to Chat (Dec, May)** – We introduced an option for *my* Social Security users to receive help from an employee via live chat.
- **Dynamic Help (May)** – We upgraded to a modern knowledgebase in the cloud; improving our ability to proactively answer online customer questions.
- **Email Us (May)** – We modernized our website’s “Contact Us” feature, which allows customers to submit general questions about SSA’s programs and services.
- **OAO iAppeals (June)** – We provided claimants the ability to electronically file a Request for Review of a hearing decision.
- **myWageReport (January, June)** – We enhanced our online wage reporting application to improve the user experience and allow disabled SSI beneficiaries and their representative payees to use the application.
- **Representative Payee (July)** – We added functionality so that representative payees can submit accounting reports online.
- **Internet Social Security Number Replacement Card (August)** – We continued to expand the availability of our online application for a replacement Social Security card to other States, bringing the total number of States in which its available to 31, plus the District of Columbia.

Data/Infrastructure

- **Continuing Death Data Improvement (March, April, May, June, July)** – We added nearly 8 million dates of death to the Death Master File (DMF).
- **Quantum Leap** – We increased the network bandwidth capacity of additional field offices, which increases computer speed and performance. Prior to upgrade, field offices have download speeds between 3 to 10 megabits per second (about as fast as a single iPhone 6 on a 4G network). The upgrade increases the download speed to 100 megabits per second. We expect to upgrade all offices by November 2018.
- **Releases on Time** – Through June, we completed 96 percent of our scheduled releases on time or early.

In addition to our systems releases, I'm proud of the work we've done to engage and learn from the broader IT community, including the government and the private sector. In June, we hosted an IT Transformation Industry Day, where we provided an overview of our modernization plan and procurement process to 205 vendors. We also met with senior staff in Johns Hopkins Applied Physics Lab to learn from their work on automated intelligence, big data analytics, and other topics.

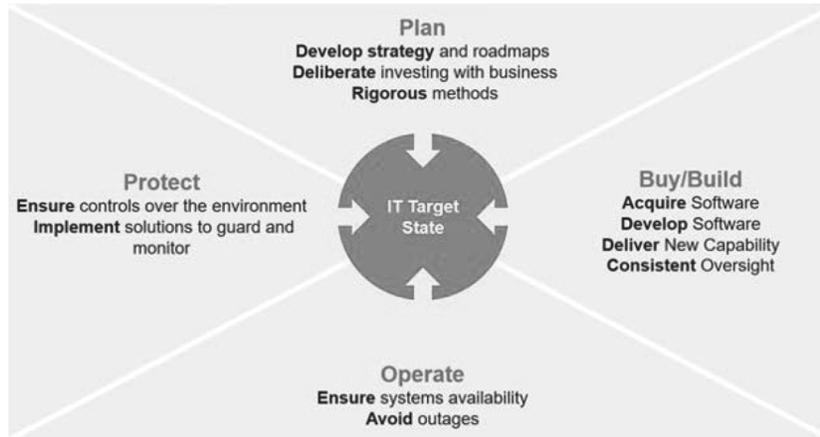
Finally, I want to give you an update on our progress in implementing Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (P.L. 115-174). As you know, this law requires us to develop a system that allows financial institutions and related entities to—after obtaining a person's consent—verify the person's name, Social Security Number, and date of birth in connection with a credit transaction.

We are working diligently on a number of fronts to implement this law as quickly as possible, including reaching out to the financial institution community as well as experts in privacy and security. We are also updating our regulations, and developing the user agreements, as well as developing the e-signature requirements for authorizing one's consent to share personal data. We are also using this opportunity to look at ways we can improve our data exchange systems and processes.

Conclusion

Information technology is vital to nearly every part of the work we do to serve the American people. Our IT modernization plan will improve the efficiency and effectiveness of our service, allow us to keep pace with changing technology and expectations, and ensure that we can continue to safeguard the sensitive information entrusted to us. We are focused on successfully implementing our IT modernization plan. We appreciate the Subcommittee's and the Congress's support.

Appendix A – Maturing IT Towards the Target State



Chairman JOHNSON. Thank you, sir. I appreciate that comment.

Ms. Stone, welcome. Please proceed.

**STATEMENT OF GALE STALLWORTH STONE, ACTING
INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION**

Ms. STONE. Thank you. Good morning, Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee. Thank you for the invitation to testify today.

SSA administers programs that result in payments of more than \$2.5 billion per day, and it holds sensitive data for more than 300 million people. SSA continues to rely on legacy coding and applications that are decades old. This is an unsustainable path.

To ensure that SSA meets its increasing service delivery demands, the agency must modernize its IT infrastructure. For many years the OIG has recommended that SSA commit to long-term strategic IT planning.

Just last year the agency issued its IT modernization plan, which is a multi-year effort to update SSA's major systems. The plan reflects investments of almost \$700 million over 5 years to support various modernization efforts. This is a significant but necessary undertaking which will need close management and monitoring. We will review SSA's progress on these plans as a part of our 2019 audit work plan.

One of SSA's major IT modernization efforts is the disability case processing system, commonly known as DCPS. With DCPS, the agency envisions a national common-case processing system for the 52 State disability determination services, or DDSs.

SSA began planning this project in 2008. Seven years later, after spending about \$350 million, the agency discontinued that effort and began developing a new version of DCPS. The agency delivered the first release of the new system to three DDSs at the end of 2016. By November 2017 employees in 10 DDSs were using the new system to process selected workloads. Soon thereafter, SSA suspended deployment and shifted its focus to systems development to address user feedback.

This year we received feedback from 120 users and found that they generally liked working with the new system, but they would like additional functionality. We also reported that participating DDSs used the new system to process about 4 percent of their total workloads. SSA plans to resume deploying DCPS soon, with a goal of delivering the system to the majority of the DDSs by the end of 2019.

SSA has spent \$101 million on the new version of DCPS, and it anticipates spending an additional \$76 million over the next 4 years. To date, the new version has been implemented at more DDSs than the previous iteration, and its estimated cost is about half of what SSA invested in the prior effort. Nonetheless, the agency still needs to address risks that may undermine successful implementation of the new system. One such risk involves convincing DDSs to adopt this technology.

For DCPS to be deployed and utilized nationwide, the project requires diligent oversight and continued user involvement. As the agency moves forward with its IT modernization, it is imperative

that it give proper attention to security. In our most recent annual audit of SSA's information security program, we identified a number of control deficiencies that may limit SSA's ability to adequately protect its systems. SSA needs to make addressing these deficiencies a priority.

Thank you for the invitation to discuss these issues. We will continue to work with the agency and this Subcommittee to address these important issues.

Finally, I want to commend the Chairman as he concludes a decorated and distinguished career in service to our country. On behalf of the OIG, thank you, Chairman Johnson, for your service, your sacrifice, and your leadership.

This concludes my statement. I will be happy to answer any questions.

[The prepared statement of Ms. Stone follows:]

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 programming 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.



Chairman JOHNSON. Thank you so much. I appreciate that comment. And thank you for your statement.

Ms. Harris, welcome. Please proceed.

STATEMENT OF CAROL C. HARRIS, DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. HARRIS. Chairman Johnson, Ranking Member Larson, and Members of the Subcommittee, thank you for inviting us to testify today on the Social Security Administration's management of IT. As requested, I will briefly summarize our work on the agency's management of IT acquisitions and operations, and the authorities of its Chief Information Officer.

As you know, SSA is responsible for delivering services that impact almost every American. And the agency extensively relies on IT resources to do so. Its computerized information systems support a wide range of activities, such as 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, software, computer maintenance, and contractor support.

SSA has long been challenged in its management of IT. Our past reports from 2004 to 2012 have highlighted various weaknesses in the agency's systems development practices, governance, and requirements management. As such, we stress the need for SSA to strengthen its IT management controls.

Between 2011 and 2018 we made 15 recommendations to SSA, aimed at improving IT management and operations in the areas of data center consolidation, incremental software development, IT acquisition strategies, and software licenses. I am pleased to report that, as of today, Social Security Administration has fully addressed 14 of the 15 recommendations. Accordingly, SSA is better positioned to more effectively manage its IT.

For example, in May 2014 we reported that SSA was one of 22 agencies lacking a robust software license management policy, as well as a comprehensive inventory of software licenses. Without these tools, agencies would not be able to systematically identify unused software and achieve savings. SSA has since established both a comprehensive policy and inventory, and is equipped to more effectively manage its software licenses.

Additionally, last year, we reported the agency lacked a complete data center optimization plan. We emphasized that without such a plan SSA might not achieve OMB's data center optimization targets or realize its expected savings. The agency implemented the related recommendation, and in May of this year we found that SSA reported the most progress among 22 applicable agencies in meeting OMB's targets.

While SSA has made noteworthy progress to improve its management of IT, more work is needed to fully address the role of its Chief Information Officer (CIO) and its policies. Various laws and related guidance assign IT management responsibilities to CIOs in six key areas. And in August 2018 we reported that, of the six areas, SSA's policies only fully address one.

Specifically, the agency's policies fully addressed the CIO's role in IT leadership and accountability by requiring the CIO to report directly to the agency head. In contrast, the agency's policies do not address the IT workforce area at all, including requirements for the CIO to assess agency IT workforce needs and develop strategies and plans for meeting those needs.

In addition, the agency's policies only minimally address the area of IT strategic planning, lacking requirements for the CIO to measure how well IT supports agency programs, and to report annually on progress in achieving goals for improving agency operations.

Accordingly, we made a recommendation to SSA to address the policy weaknesses in five management areas. In response, the agency agreed, and indicated it planned to implement the recommendation by the end of this month.

It would be especially important for SSA to ensure that the policies for its CIO responsibilities are robust, given its high turnover of CIOs. Since 2004, the average tenure of SSA's CIO is 1.8 years. Our work has shown that a CIO should stay in office for 3 to 5 years to be effective, and 5 to 7 years to fully implement major change initiatives in large, public-sector organizations. If SSA fully implements our recommendation, it will be better positioned to attract and retain high-quality CIOs when there is a leadership vacancy, while also maintaining continuity of IT operations when leadership changes occur.

That concludes my statement, and I look forward to addressing your questions.

[The prepared statement of Ms. Harris follows:]



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

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.

September 2018

INFORMATION TECHNOLOGY

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

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.

¹For 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).

²GAO, *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.

⁴GAO, *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.

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

⁶For 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 amendments⁷ 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.

⁷Title 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.

⁸Social 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

⁹See, 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).

¹⁰SSA 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

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

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

¹³Exec. 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

¹⁴GAO, *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 data 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

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

¹⁶GAO, *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 2018¹⁷ 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

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

¹⁸The 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.

¹⁹OMB 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.

²⁰OMB'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

²¹40 U.S.C. § 11319(b)(1)(B)(ii).

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

²³GAO, *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

²⁴OMB, M-15-14.

²⁵OMB'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.

²⁶OMB 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.

²⁷The 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

²⁸GAO, *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.

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

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

³¹The 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

³²GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-83 (Washington, D.C.: Aug. 2, 2018).

³³These 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 Eyer.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



Chairman JOHNSON. Thank you. Thank you so much.

As is customary for each round of questions, I will limit my time to 5 minutes and will ask my colleagues to also limit their questioning time to 5 minutes, as well.

Mr. Mathur, modernizing Social Security's IT is a huge challenge. How are you making sure that this project is done on time and does not have cost overruns?

Mr. MATHUR. Chairman Johnson, thank you for that question. Our IT modernization plan, as you noted, we published in October of last year. As I noted in my opening remarks, we are on schedule and we are on budget.

We have an accountable executive for the IT modernization plan, he is sitting right here, behind me. And we have accountable executives for every initiative within the IT modernization plan.

We have a number of controls and governance in place with oversight, and this really is a management effort for us to make sure that we are constantly delivering values.

I will close with the following point when it comes to modernization and what we are doing: Our approach to this is to make sure that whatever we are working on within the modernization effort is very focused on the customer, whether it is the front-line employee or a member of the public. And being able to deliver that value early and often, and then making sure we have that feedback loop, is an important way to make sure you are on track. That is the way, that is the private-sector industry standard to be able to have that quick feedback loop.

Chairman JOHNSON. Have you had any complaints so far?

Mr. MATHUR. I would say that our users, especially our business customers, have been pleased with the progress we have been making. And the complaint, if there is one in that regard, is go faster. How do we go faster? How do we deliver more value? So that has been the focus for us.

Chairman JOHNSON. Well, in your testimony you stated the estimated cost for the disability case processing system was \$177 million. Isn't that an increase from the previous estimates that you gave us? And why did they increase?

Mr. MATHUR. Sir, as you may know, DCPS2 is currently in 10 DDSs, and it is soon to be 14. We are talking with another 34, in terms of rollout to those 34 DDSs.

The DCPS2 project is grounded in making sure it is delivering value, and working with these DDSs that are already using it. And so we have a DCPS steering committee, which consists of State administrators and many of the States that currently use this DCPS2 product. As we get feedback, and as we have already received feedback on what additional functionality was needed in the product, we have rolled that into the road map. And that was the basis for that increase in cost.

Chairman JOHNSON. Do you expect any more increases, or are you going to stay on target?

Mr. MATHUR. We are staying on target, sir. We are always managing that road map, and what that product lineup looks like.

Chairman JOHNSON. And you don't expect any more increases in the future?

Mr. MATHUR. We are managing that product very closely. I am personally involved, as well as agency leadership. And I will say that, in constantly talking with the users, we are managing what we deliver and when we deliver it early and often, as I mentioned. If the user requirements end up changing, we will modify the road map. At this point I think we have a road map that I am very comfortable with, and that is what we will deliver on.

Chairman JOHNSON. The modern approach to IT development can make it hard to tell if a project is on track, because requirements change as development progresses. As CIO, how do you make sure that the modern development projects you oversee are going to stay on track?

Mr. MATHUR. I would refer to my private-sector experience, which is that we are looking for value. That has been the mantra that we have been following when it comes to DCPS2 or our IT modernization efforts. So, as long as we are having the conversation on a regular basis with our end users, that is how we make sure we are delivering value and we stay on track.

There is a quick example I would give you, if I could, sir. If you were remodeling your kitchen, and your contractor said, "Come back to me in a year and I will let you know what it looks like," you are probably not going to get what you want. But if you were able to look at it every day, every week, you can probably tweak the direction. That is the model we are using when it comes to modernization.

Chairman JOHNSON. So what you are telling me is you are staying on top of it.

Mr. MATHUR. We are.

Chairman JOHNSON. Thank you.

And, Ms. Harris, what are your thoughts on the project?

Ms. HARRIS. Well, I think, regardless of the approach that you take, whether it is a more modern, agile approach, or the more traditional waterfall approach to software development, you are always going to need sound project management. And that management is just going to look different in this more modern, agile approach.

Agile essentially means you take these traditional, monolithic, large-scope projects, and you break them out into these small increments, so that you are delivering software every 6 to 12 months.

I am glad to hear Rajive talking about a road map, because in this modern approach that is your baseline for measuring progress, from a cost and schedule perspective as well as the performance and the delivery of what is being planned for.

And so, as long as Rajive and his accountable executive are measuring against this road map, that is how we are going to be able to tell whether progress is being made as planned.

Chairman JOHNSON. Well, are we on track?

Ms. HARRIS. Well, I can't speak specifically to DCPS, but I—you know, he is using at least the right words, in terms of what you would expect in a well-managed program, particularly that road map.

Chairman JOHNSON. That is what we all have to do, is use the right words, right?

[Laughter.]

Well, I recognize you, sir.

Mr. LARSON. Thank you, Mr. Chairman.

Mr. Mathur, you used the term “person-centric” in your opening remarks, and I couldn’t agree with you more, especially with 10,000 baby boomers a day becoming eligible for Social Security. How do you carry that out from an IT perspective for both the citizens we serve, as well as the employees that, you know, have to make sure that, as they deal with their day-to-day work with delivering Social Security, this transpires?

Mr. MATHUR. Congressman, person-centric is an important term among a number of other terms that we use. It is a philosophy. And I will describe it in the following way.

Today, when a member of the public walks into a field office, they will get great service, and we know that. But the representative on the other side of the desk is looking through multiple systems, multiple screens, making sure that they get the right information to serve that customer. That takes time. There is a possibility for errors. And it is confusing, right?

This person-centric approach and the example I will use is that next fiscal year—this fiscal year we are looking to deploy the first version of the universal customer view, which is a single portal for everything that a technician may need to know about a member of the public that is coming in. So you can see your transactions, you can see your history with the SSA. That is the—that is where the ideal is, correct? That is person-centric.

So if you are—if we are engineering that experience, that business process for that end user customer and the front-line employee, we will then be able to make sure that process works and the technology underlying the process works.

Mr. LARSON. I had a number of conversations on the Committee, but specifically with Representative Schweikert, and I wanted to get your opinion on block chain as a technology, and how you see—if you do see—that as having an impact as we move forward, in terms of the delivery of service, and how that might be utilized, and if Social Security is considering that.

Mr. MATHUR. That is a great question. I would say block chain, as well as other technologies, these are things that I am tracking, we are tracking. We are not using it yet. We are in the early stages of looking at it.

JPMorgan Chase, for example, is using some version of it, again, relatively early. It has promise. It has promise in various applications. I can certainly give you some examples. But it is something we are tracking.

Mr. LARSON. Well, could you get me some examples? Because this is a conversation that is ongoing. And certainly, we want to do everything that we can to try to both look forward and streamline our process, make it more person-centric, but also hopefully utilize the technology that is at our disposal. We wouldn’t want to overlook something that could be a game-changer and also, from a cost-effective and efficient standpoint, be helpful to us.

Mr. MATHUR. Sure. One example is a provider directory. So we are using—today the medical providers that are—the directories or the classification of medical providers all over the Nation is always changing, it is always in flux, there is always a chance for error,

whether it is contact info, whether they are still licensed or not licensed. These are—that is a changing piece of information that our technicians rely on to be able to contact these providers for records, et cetera.

Using block chain, which would distribute the information and let the local providers in a secure way still be able to update their provider records, that we would then be allowed to use, would be an example to have the most up-to-date information about providers at any given time. If we are responsible for it, you know, we have enough to do, and it is tough to get it all right, in that regard. But if the people who are responsible for that data can update it when they need to do it securely, then we can get that information. That is one example.

Mr. LARSON. One of the over-arching—this is for all the panelists—one of the over-arching concerns that this Chairman has always been focused on is certainly identity theft, as it is related to Social Security. What does Congress need to do, in terms of assisting you, and what is the SSA doing with respect to making sure that people's identity is protected?

Mr. MATHUR. Congressman, protecting individuals' identifiable information is integral to what SSA does. It is part of what the agency started when first assigning the SSNs. We take it very seriously, when it comes to protection of Personally Identifiable Information (PII). We have a plan in place to execute on NIST Special Publication 800-63-3 guidelines, which are guidelines for digital identity. And that will allow us to be able to protect—continue to protect the public's PII. We have a number of controls in place now, but we always have to stay ahead of this issue.

Mr. LARSON. Ms. Harris, what do you think about that?

Ms. HARRIS. I can't speak specifically to SSA, but certainly cyber security and the protection of personally identifiable information is one of the key high-risk areas on GAO's top high-risk list. And that is certainly something that our Comptroller General has spoken quite a bit about, as, you know, one of the top priorities that the Federal Government should be focused in on.

Mr. LARSON. Ms. Stone.

Ms. STONE. I will take a slightly different angle on this and say that there have been security breaches where personally identifiable information has been confiscated by guys who want to commit fraud. The focus at SSA has to be on authenticating the individuals that want to come in and do business with the agency to make sure that the person applying for those benefits is actually the real number-holder.

Mr. LARSON. Thank you.

You wanted to respond further?

Mr. MATHUR. I would add that identity theft and knowing who you do business with, as we do more and more digital services, this is a very important problem, certainly—it is a societal problem. And we are working with other Federal agencies, as well, so that there is a way to be able to counter this across Federal Government and, frankly, with the private sector, as well. We all have the same needs when it comes to identifying that individual.

Chairman JOHNSON. Thank you.

Mr. Bishop, you are recognized.

Mr. BISHOP. Thank you, Mr. Chairman. And if I could, I would like to begin by building on the words of gratitude and reverence for your service to this country and for all that you have done: Your service to Congress, your service to this Subcommittee, and all that you have done for those who depend on Social Security in this country, for your service to country as a hero in the United States Air Force.

I got into this job 1½ years ago, not—a little bit more than that, actually, but it seems like yesterday, and I did it because—I left the private sector because I believed in my country. I am a student of history and government. I felt as though I had to do something for my country, and I believe in my country, I love my country. And I am so grateful to be able to serve here, so honored to serve here, but it really blows my mind to think that I have the opportunity to serve with someone like you. And the honor to know you, to be a part of this Committee has been just incredible for me.

So, sir, I—your country thanks you, I—we all thank you for all that you have done. And thank you for making this experience something I will never forget.

I just wanted, if I could, then, to build on the theme that we have been talking about with regard to customer-centric and end user customer and front-line employee. I have said this before, and we have been talking about it before, because I had the opportunity to introduce, with Ranking Member Larson, the Improving Social Security's Service to Victims of Identity Theft Act, which I think is so very important. We—all of our constituents talk about identity theft and ways that we can improve that.

I am encouraged to hear what you have been talking about with regard to your IT projects. Mr. Mathur, I was wondering if you could just share with me. When it comes to IT projects like this at SSA, how do you determine who is responsible for the project's success or failure, and how do you hold them accountable?

Mr. MATHUR. Thank you for that question. As I mentioned, we do have accountable executives, starting at the top and then laddering down for the IT projects that we have.

When it comes to modernization projects, for example, we have a business and IT lead that are jointly responsible for that effort. Regardless of what kind of effort it is, there is always a business owner that we need to make sure we are catering to, and there is an IT executive that is managing that effort.

Accountability is an important part of our approach. I continue to meet with all the major investments that we make, and my leadership team does, as well. We have direct oversight over the efforts that we have, when it comes to these major projects.

It is a continuous management need to be able to hold people accountable, to make sure executives are meeting those dates, and delivering value.

I think the key thing that I would say is that the focus on value is what helps ground me and what I would like to see in every IT project. One of the things I have said internally to our teams is we are going to be communicating horizontally, as opposed to up the chain of command, across, and down. In a large organization that happens frequently, so you have to have the business customer in

the room so they can hold each other accountable, so that they are accountable to each other and to us.

Mr. BISHOP. So that road map you are working on, and the organization chart of the folks that are working on that road map, you are all aware, you are all working together on that same road map. Are you—do they have a direct line of communication with you? Is that how that works? And is this process kind of a Gantt chart within the road map, where you have certain tasks to finish within a certain amount of time?

I am just interested to know what the management process is.

Mr. MATHUR. So the road map is—it is a multi-year road map. The road map is developed with the business and IT owners together, not just one group or the other, focusing on multiple deliverables early and often, always delivering a piece of capability—the software, whether you buy it or whether you build it.

The level of dialogue that we have—we have introduced a function called product management that is—as part of our—it is a product orientation for how we look at anything. It is customer-driven. Whenever you are delivering a capability, you are looking at it as a product and service.

So that role, plus the project manager, are managing the day-to-day, and then making sure that the business and IT users and the leadership is also apprised of it.

Mr. BISHOP. Mr. Mathur, thank you. And I have several other questions.

I know that we have limited time, so I will yield back the time, Mr. Chairman.

Chairman JOHNSON. Thank you.

Mr. BISHOP. Thank you.

Chairman JOHNSON. Mr. LaHood, you are recognized.

Mr. LAHOOD. Thank you, Mr. Chairman. And I would also like to thank you for your sacrifice in Vietnam, thank you for your service in the Congress here. Your examples of humility and sacrifice will stay with all of us. And while you may be returning and moving on, your legacy will live on because we will be back here in the Sam Johnson room many times, and we will be thinking about you often and the example that you left for all of us.

So thank you, sir. It is an honor to serve with you.

Chairman JOHNSON. Thank you.

Mr. LAHOOD. Mr. Mathur, during the original rollout of the DCPS beta, my State of Illinois had some challenges with functionality. Since the success of DCPS2 depends on States voluntarily adopting the system, what steps has SSA taken to encourage adoption, particularly to States like mine who had challenges last time?

Mr. MATHUR. Congressman, DCPS2, as you mentioned, has had a successful rollout to 10 States, with 4 to come, as I had mentioned earlier. We are developing the capabilities for DCPS2 in lock step with what the steering committee and the business users are looking for, the DDSs are looking for, including the State of Illinois.

And I would say that, over time, as more and more capabilities get developed, I can't imagine why a State wouldn't want—or a DDS wouldn't want to use that capability, since they helped design it. The system is being designed by users for users.

So my hope is that—and my goal is a nationwide, common-case processing system, and that is where we think DCPS2 can get us.

Mr. LAHOOD. And what happens—or what are the consequences if a State doesn't use the new system?

Mr. MATHUR. Well, I think we would have to address that when and if that time comes. My hope is that it wouldn't come, because the product is going to meet their needs.

Mr. LAHOOD. Thank you. Let me switch to another subject, Mr. Mathur.

Federal laws and regulations have been pretty clear that agencies should first look to the private sector for solutions to their IT needs. But communication between the SSA and industry hasn't always been easy. How does SSA engage with industry to identify potential IT solutions?

And as a followup to that, can you expound or comment a little bit upon the IT Transformation Industry Day that I know you recently hosted?

Mr. MATHUR. My bias is toward buying and not building. As part of our investment process, whenever we are looking at any sort of need that we are trying to fulfill with technology, we must look at external solutions, other government agencies, shared solutions, and then, of course, the internal solution.

So we have to have a bias toward finding out what we can buy externally, and then use it internally. That is the way I am wired, that is what I would like to continue to do, and that is part of our process, it is part of the policy that we have in place.

The IT Industry Day that we had back in June, we had over 200 members of industry that were part of the session. We had five different topics. It was great—it was a virtual industry day. It was a great model, the first time we had ever done it, where we presented some ideas on what we were looking for. We received some good questions, some good feedback, some followup from industry. We hope to repeat that process.

Recently we also met with Johns Hopkins for block chain and for AI, as another example of outreach. I mean, this is something that we need, we continue to do and get better at, but we need to do more of it.

Mr. LAHOOD. Well, thank you. We look forward to working with you on that.

Those are all of my questions, Mr. Chairman.

Chairman JOHNSON. Thank you.

Ms. Sánchez—

Ms. SANCHEZ. Thank you, Mr. Chairman. And before I begin I just want to add my voice to those who have already thanked you for the many years of your service to the Congress and on this Committee.

Chairman JOHNSON. Thank you.

Ms. SANCHEZ. We are sad to see you go.

I want to thank our witnesses for being here today. It kind of baffles me that one of the richest countries in the world that is at the forefront of technological innovation has inadequate and outdated technology operating within the walls of its government. So I am particularly pleased that the Social Security Administration is making such progress with its IT modernization plan.

I know that you are investing several hundred million dollars to update the existing operating system and, clearly, it is long overdue if you guys have equipment that you are using that dates back to the 1950s. No doubt, just having that older technology is tough to maintain and slow to operate. And obviously, it can be very inefficient, I guess, and wasteful, even.

For example, I know that SSA spent about \$1.6 billion on IT in fiscal year 2018. That is over 10 percent of its total operating budget. And that is \$1 billion that went into just maintaining an out-of-date operating system. So I think it is high time that we make an investment in our technological infrastructure that will, hopefully, improve service and security, as well.

My question is for Deputy Commissioner Mathur. What sort of efficiencies do you think are going to be realized through IT modernization? And most specifically, is it going to help in terms of being able to get faster decisions and processing of benefits for constituents?

Mr. MATHUR. Thank you for that question. The efficiencies that we are—let me give you one example of one efficiency that we think we can get to.

I talked earlier about the universal customer view, which is a single portal which allows our technicians to see interactions that a member of the public has had with SSA, any communications they have had, and it allows them to do this by not having to thumb through many different screens, but to just get to everything all in one place.

In fiscal year 2019 we are also going to be coming up with a minimal viable product for a pre-claim system. And what that is is a single claims path, regardless of the type of benefit that you are looking for.

Today, when you walk into a field office or are interacting with a technician, they are figuring out what they need to—what you may be eligible for. The pre-claim system is a single way for them to be able to ask the right questions and be able to determine, in an efficient way, with appropriate branching and logic, what you may be eligible for, as a member of the public.

So that is one small example, but an important one.

Ms. SANCHEZ. So I am assuming it will result in faster processing times and, you know—

Mr. MATHUR. It will be more efficient.

Ms. SANCHEZ [continuing]. More efficient, you know, processing of benefits.

Mr. MATHUR. Yes.

Ms. SANCHEZ. Okay, excellent. I know that the Social Security Administration keeps records of people's personally identifiable information. And obviously, in this increasingly high-tech world, a concern that we all share is the safety of protecting that information.

I am guessing—but I would like to hear from you—that older technology probably is more vulnerable to breaches in the system. So is the IT modernization going to help strengthen the agency's ability to safeguard that personal information? Will that make our information safer, as well?

Mr. MATHUR. We are always staying ahead and staying on top of the security of the systems. As someone mentioned earlier, the continuity of operations is paramount for the agency, in making sure that they are secure. It is certainly important.

In terms of IT modernization, security is built in. It is not retrofitted after the fact. So as we are going through the development of these various efforts—cyber, needs, authentication—assuming that somebody is going to be interacting with us on the Internet, which is different than 20, 30 years ago, where they might be calling in, those assumptions of the Internet and better security needs are now built into the process.

Ms. SANCHEZ. So will that result in—

Mr. MATHUR. That will result in—

Ms. SANCHEZ. Better safeguards for the—

Mr. MATHUR. Better, more flexible safeguards, yes.

Ms. SANCHEZ. Perfect. Those are all the questions I have. I yield back.

Chairman JOHNSON. Thank you.

Mr. Schweikert, you are recognized.

Mr. SCHWEIKERT. Thank you, Mr. Chairman. You know, it is hard to think of this room without you sitting in that chair, chairing a hearing. For those of us who hope to stay on this Subcommittee in the future, you know, we will always look up and see your name there.

Thank you for your incredible service to all of us—as the phone goes off. But thank you. You know, my wife, this summer, actually read your book and you brought her to both tears and joy. So it is a recommendation for everyone.

Ms. HARRIS, simple question, and just conceptually, should the IRS actually even own its own servers? In a world where encrypted cloud is becoming ubiquitous, is that a vision for you?

Ms. HARRIS. I am sorry, sir. We have—I have personally not done work at the IRS, so I am not in a—I am not the best expert to weigh in on that.

Mr. SCHWEIKERT. Okay. But then how about for Social Security?

Ms. HARRIS. Within the Social Security Administration I also have not done that specific level of work. So, unfortunately, I—

Mr. SCHWEIKERT. Okay, I was—

Ms. HARRIS [continuing]. That is outside of the scope of the work that I have done.

Mr. SCHWEIKERT. All right, sorry. I was going to sort of go through the larger agencies.

For anyone, has there been studies for Social Security, Medicare, or others to actually make the decision is maintaining their own server farms still appropriate?

Mr. MATHUR. I will take a crack at it. We have a Cloud Smart policy when it comes to any capabilities that are being developed. So as we are considering what the hosting is going to be for a particular software application, it makes sense, by default, to think about the cloud, but making sure that it is the right application, that it has the right profile for safety, for security, and that you are not just putting something on the cloud because—

Mr. SCHWEIKERT. But I thought most of the safety and security concerns have—I mean, they are now a few years old. And the ability to encrypt and split and collocate—

Mr. MATHUR. It is a fair point. It is the application, but it is also the data behind the scenes that need to be—that these applications sometimes need to access. So the location of the data may help drive where the application gets hosted, whether it gets hosted on the cloud or not.

The point I would make is that it doesn't—it is not, by default, hosted within our data center—it shouldn't be hosted by default by the government. It could be hosted in a private cloud, or it could be hosted in a public cloud. I mean, there are a number of different stages of decisionmaking that it could and should have, and that is how we are approaching it.

Mr. SCHWEIKERT. Okay. All right. If you have something I can read, or something I—

Mr. MATHUR. Sure.

Mr. SCHWEIKERT. Because it is not a particularly satisfying answer.

Could we actually sort of do a quick walkthrough of the legacy systems? And when will there be the last day that you will be running, you know, functionally, COBOL with a—in front of it—you know, when will those legacy systems be gone, that legacy code?

Mr. MATHUR. Congressman, our IT modernization plan substantially will make a dent in and remove legacy technology, legacy code. Not just COBOL, but other legacy codes, code types—we have assembler, and others.

Here is the challenge we are facing, which is we—continuity of operations, making sure that you can deliver those services when somebody walks into the field office or calls the tele-service center, that has to always be on and operational—

Mr. SCHWEIKERT. But wasn't the original plan to run parallels and then do the transfer over?

Mr. MATHUR. That is exactly right.

Mr. SCHWEIKERT. And so shouldn't that actually mean there is a target switch date, if you are running parallels?

Mr. MATHUR. So the plan is to have a parallel operation, and once we have launched, once we have put something in the market and it works, at that point we start retiring, right?

It is not—it doesn't—and it happens—it is rolling thunder. So we will be developing capabilities, launching it, launching them, having frontline employees use them, have members use them and then do the migration. So it is not that we will be retiring at one specific date. It will be happening throughout the plan.

Mr. SCHWEIKERT. So back to the original question. When do you see, in your Utopian—techno-Utopian future, when, you know, the legacy codes and the bolt-on are gone?

Mr. MATHUR. So I see that the modernization plan will substantially remove that. That is a 5-year plan—

Mr. SCHWEIKERT. Okay, so is the goal in 5 years to no longer have legacy code, or is it 25 years?

Mr. MATHUR. I—

Mr. SCHWEIKERT. I mean, what is your best guess?

Mr. MATHUR. I think it is going to be substantially gone in 5 years, but it won't be 100 percent gone in 5 years.

Mr. SCHWEIKERT. Okay.

Mr. MATHUR. Because in some cases it may not make sense for us to migrate an old legacy technology to the modern—it may not make business sense. And that analysis, to be able to look at—excuse me.

Mr. SCHWEIKERT. Okay, and I am so sorry. We are in the last few seconds.

My friend actually spoke about my fixation on block chain and distributive ledger, you know, and that future for when everyone who is a potential beneficiary can pick this up and basically track their own files, see who has looked at their files, when did they actually move any paper, and yet have levels of permission and encryption and security.

And where I was going to go before is my sort of techno-Utopian fantasy of being able to see my benefits, I could see my IRS tax records, I could actually see my military discharge, I could see everything sort of in a common portal. And I fear a lot of my big agencies with massive data haven't really begun to talk to each other about ever sort of unifying a platform, probably on a distributive ledger, with the proper encryption, and providing those services to the American public.

So that is sort of a last—and, Mr. Chairman, thank you for your tolerance.

Chairman JOHNSON. Thank you.

And, Mr. Rice, you are recognized.

Mr. RICE. Thank you, Mr. Chairman, and thank you for the years of being able to learn from you, and your mentorship. And I appreciate so much your service to our country.

I am just frustrated with the progress on the technology improvement at Social Security. I think one of the big problems is maybe we haven't done a great job of holding people accountable. But, Ms. Harris, you mentioned the road map, and that a road map is a good start, and that—but you also said you weren't familiar with it. So you don't work with Social Security?

Ms. HARRIS. No, we do audits of their IT management and operations. We have received their IT modernization plan, and we have taken a look at it. On the surface, it looks very good, but we have not done the detailed dive into it to look at the meat of it, at least not at—at least not yet.

Mr. RICE. Why? I mean, you are the Government Accountability Office. You are supposed to hold people accountable. They send you the road map, it seems to me like you would have somebody watching them every month, right? Why don't—you haven't done a detailed dive into it?

Ms. HARRIS. Well, we do have limited resources, and the work that we do is driven by congressional request and mandates. And because we have not been mandated to do that detailed dive, we simply cannot do that work.

Mr. RICE. So you are the Government Accountability Office, but you are not going to hold them accountable.

Ms. HARRIS. Well, we do hold them accountable in terms of the recommendations that we have made. We do, over a 4-year period

after the recommendation is made, ensure that we—you know, we continue to monitor them to determine to what extent they have implemented our recommendations.

Mr. RICE. Ms. Stone, you said that you are trying to migrate to a single case management system, right?

Ms. STONE. The agency is.

Mr. RICE. Yes, ma'am.

Ms. STONE. I apologize. The agency is.

Mr. RICE. Yes, ma'am. How many case management systems do they have now?

Ms. STONE. Each of the 52 DDSs previously had their own individual systems, which gave rise to the need for DCPS.

Mr. RICE. And they don't talk to each other, and you can't move cases back and forth between them. So it is remarkably and horrifically inefficient, right?

Ms. STONE. It is complicated.

Mr. RICE. So you said you tried to roll one in 2008. You did that for 7 years, but it didn't work. You pulled it and you started a new one, right? And you spent \$300 million along the way. Isn't that what you said?

Ms. STONE. Yes, sir. But just as a clarification, OIG itself did not do that, but those were decisions of the agency.

Mr. RICE. Yes.

Ms. STONE. And, as a part of our audit work, we identified those scenarios.

Mr. RICE. Okay. So you are supposed to be holding them accountable, too, right?

Ms. STONE. Yes, sir.

Mr. RICE. You are there, right? You are in Social Security. So what is the timeline? Okay, you said you put this new case management system in place in 2016 in—what did you say, three offices?

Ms. STONE. In three DDSs, yes.

Mr. RICE. How many DDSs do you have?

Ms. STONE. Fifty-two.

Mr. RICE. You have fifty-two DDSs. So you put it in place in three. Which three were those?

Ms. STONE. I don't have those.

Mr. RICE. Okay. All right. So you tried it in three for a little while. How long?

Ms. STONE. I will defer to—

Mr. RICE. How long?

Ms. STONE [continuing]. The agency.

Mr. MATHUR. How long did we—

Mr. RICE. How long did you try it in those three DDSs?

Mr. MATHUR. We are trying and continue to try them, and then—they are using them now.

Mr. RICE. Okay.

Mr. MATHUR. In fact, now it is 10, soon to be 14.

Mr. RICE. I thought you said you stopped using it. I thought you said you tried it, you pulled back, you asked for feedback, and then you were going to go in again. That is what you said. That is what you said.

Ms. STONE. May I clarify?

Mr. RICE. Yes, ma'am.

Ms. STONE. In 2016 SSA rolled out to three. In 2017 SSA rolled out to ten. And instead of deploying DCPS to additional DDSs, SSA stopped further deployment so that they could look at modifying the software based on feedback from those DDSs that were currently using DCPS.

Mr. RICE. Okay. I have about a million questions—

Ms. STONE. Is that a correct—

Mr. RICE [continuing]. And I have 1 minute. But this case management software that you are using, is it off the shelf or is it something you are developing?

Mr. MATHUR. We looked at market options, Congressman. This is an in-house developed—the requirements for the DDSs and our business process in general is a very complex—there is nothing out there that is going to be plug-and-play, in terms of off-the-shelf. So we have looked at market options, we are doing market research right now, as well.

Mr. RICE. I really don't think that what you are doing is all that unique. I really don't. And I don't know why in the world you couldn't find something off the shelf.

Who is developing this? Is it the IT department that is overseeing the COBOL systems?

Mr. MATHUR. It is our—it is a combination of our—it is our business partner, internal business partner, as well as our IT group.

Mr. RICE. What does that mean, "business partner"?

Mr. MATHUR. The user that will eventually use the software. They are like—

Mr. RICE. So—

Mr. MATHUR. They are hand-in-hand—

Mr. RICE. You are talking about one of the DDSs?

Mr. MATHUR. No, it is an internal organization that is working with the DDSs and the—

Mr. RICE. Okay, what is the name of that—

Mr. MATHUR. Operations.

Mr. RICE. Operations. So they are not a business partner, they are part of the government.

Mr. MATHUR. They are part of the government, yes.

Mr. RICE. Yes, okay. And one last question, Mr. Chairman. I know I am going over, but who is making these decisions? I mean, do you have any kind of outside consultant, or do you guys just do this in-house? Are you all making these decisions about if you are going to design it yourself or if you are going to buy off-the-shelf? And if you are going to buy off-the-shelf, who the vendor is going to be?

Are you all just doing that in-house, or do you have somebody who really, you know, is in this business of IT trying to help you with this?

I hope, please, God. Tell me you do.

Mr. MATHUR. We have—we do have expertise that we use.

Mr. RICE. In-house is what you are—

Mr. MATHUR. It is in-house.

Mr. RICE. Okay.

Mr. MATHUR. It is in-house experts.

Mr. RICE. Okay.

Mr. MATHUR. It is private-sector expertise that—as well as government expertise.

Part of our process is to look at these options. That is part of what we have to do, and that is one of the things that I have made sure is part of our policy.

Mr. RICE. Okay. I would like to see a list of the major systems that you have, that you want to replace, and I would like to see a timeline for that.

I mean, I heard Mr. Schweikert trying to pin you down on when you thought you would be rid of COBOL, and I heard you dance for a minute-and-a-half on not answering his question, because you don't want to pin yourself down.

But part of our job—and I am not trying to be a smart aleck—part of our job is to hold you accountable. I don't hear her holding you accountable. I am not sure I hear her holding you accountable. Part of our job is to hold you accountable. And I want you to tell me what your problems are, how you are going to fix them, and what the timeline is going to be to get that done.

And I don't expect you to give yourself unreasonable timelines, but it has to be something that we can hold you to, rather than this fuzzy dancing around, "Well, we are not sure," and "We will get rid of most of it by this date."

Mr. MATHUR. May I respond? We have a plan. I think the—in your opening remarks, a big need is, in fact, having a strategy, having a plan. We have a plan and a road map that is 5 years. That is a substantial amount of time that will get us substantially there to removing a lot of this legacy software.

And the removal of the software, the removal of the technology, the legacy technology, is going to happen as we go through the plan. It is not going to be at the—there is no one final end date, but there is an important—there are many wins that are happening all the way through. Every time we roll something out, we retire. Roll something out, we retire. That repeated phenomenon is what you are going to see, and that is what we are holding ourselves accountable for, as well.

Mr. RICE. I am so sorry. One last yes-or-no question. Are you still using any magnetic media?

Mr. MATHUR. I believe we may be, but it is not part of our core. But I can get you an answer for the record, sir.

[The submission of Mr. Mathur follows:]

Insert Page 33 Line 8

Social Security is still using magnetic tape at the National Support Center and the Second Support Center. However, in 2013 we began migrating away from the use magnetic tape for our main applications. The agency currently uses magnetic tape to support offsite, business continuity, and local backups. The Electronic Vault (E-Vault) project will enable us to decommission all usage of magnetic tape and provide an all virtual tape footprint for these backups by the end of calendar year 2019.



Chairman JOHNSON. Is he done?

Mr. LARSON. He is done.

Chairman JOHNSON. Well, that was a good line of questions. Thank you for them.

You know, Social Security's IT is critical to providing Americans with the service they expect and deserve. And while Social Security has taken steps to modernize its IT programs, there is still work to be done, which is obvious after those questions.

Social Security also needs to do a better job using the private sector to keep costs down and projects on schedule. Social Security's IT is too important not to get it right. Americans want, need, and deserve no less.

I want to thank our witnesses for their testimony. Thank you for being here. Thank you also to our Members for being here, and thank you to everybody who has helped this Subcommittee accomplish so much over the years.

With that, the Subcommittee stands adjourned.

[Applause.]

[Whereupon, at 12:16 p.m., the Subcommittee was adjourned.]

[Questions for the Record follow:]

Congress of the United States

U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS

1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625

Washington, DC 20515-0518

<http://waysandmeans.house.gov>

RICHARD E. NEAL, MASSACHUSETTS, RANKING MEMBER
 SANDER M. LEVY, MICHIGAN
 JOHN LEWIS, GEORGIA
 LLOYD DOGGETT, TEXAS
 MIKE THOMPSON, CALIFORNIA
 JOHN B. LARSON, CONNECTICUT
 FARR, BLUMENBERG, OREGON
 RON KNOX, WISCONSIN
 BILL PASCRELL, JR., NEW JERSEY
 JOSEPH CHROWLEY, NEW YORK
 DANNY K. DAVIS, ILLINOIS
 LINDA SANCHEZ, CALIFORNIA
 BRIAN HIGGINS, NEW YORK
 TERRI SEWELL, ALABAMA
 SUZAN DUBBIE, WASHINGTON
 JUDY CHU, CALIFORNIA

BRANDON CASEY,
 MINORITY CHIEF OF STAFF

KEVIN BRADY, TEXAS,
 CHAIRMAN

SAM JOHNSON, TEXAS
 DEVIN NUÑEZ, CALIFORNIA
 DAVID G. REICHERT, WASHINGTON
 PETER J. ROSKAM, ILLINOIS
 VERN BUCHANAN, FLORIDA
 ADRIAN SMITH, KANSAS
 LYNN JENKINS, KANSAS
 ERIC PAULSEN, MINNESOTA
 KENNY MARCHANT, TEXAS
 DIANE BLACK, TENNESSEE
 TOM REED, NEW YORK
 MIKE KELLY, PENNSYLVANIA
 JIM RENACCI, OHIO
 KRISTI NOEM, SOUTH DAKOTA
 GEORGE HOLDING, NORTH CAROLINA
 JASON SMITH, MISSOURI
 TOM RICE, SOUTH CAROLINA
 DAVID SCHWEIKERT, ARIZONA
 JACKIE WALORSKI, INDIANA
 CARLOS CURBELO, FLORIDA
 MIKE BISHOP, MICHIGAN
 DAWN LUKASO, ILLINOIS
 BRAD R. WENSTRUP, OHIO

GARY J. ANDRES,
 STAFF DIRECTOR

October 18, 2018

Carol C. Harris
 Director, Information Technology Management Issues
 U.S. Government Accountability Office
 441 G Street, NW
 Washington, DC 20584

Dear Ms. Harris:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the September 27, 2018, hearing entitled "The State of Social Security's Information Technology." In order to complete the hearing record, I would appreciate your response to the following:

1. How critical is effective leadership and accountability to the success of major information technology (IT) projects?
2. What steps can the Social Security Administration take to make sure that long term IT investments stay on track when leadership changes?

I would appreciate your response by **November 1, 2018**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to alex.stepahin@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,



Sam Johnson
 Chairman
 Subcommittee on Social Security



October 30, 2018

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives

Subject: GAO Responses to Questions for the Record on the September 27, 2018 Hearing on The State of Social Security's Information Technology

Dear Mr. Chairman,

This letter responds to your October 18, 2018, request that I reply to additional questions arising from the Subcommittee on Social Security hearing on The State of Social Security's Information Technology. This enclosure provides my responses.

Should you or your staffs have any questions on the matters discussed in this letter, please contact me at (202) 512-4456 or harriscc@gao.gov.

Sincerely yours,

Carol C. Harris
Director, Information Technology

Enclosure

House Committee on Ways and Means
Subcommittee on Social Security

Committee Hearing:
The State of Social Security's Information Technology

Questions for the Record

Questions for the Record from Sam Johnson, Chairman, Subcommittee on Social Security

1. How critical is effective leadership and accountability to the success of major information technology (IT) projects?

Effective leadership and accountability is essential to the success of IT projects. In an October 2011 report, we identified a number of common factors that had been critical to the success of selected IT investments in achieving their respective cost, schedule, scope, and performance goals.¹ Among these factors, we noted that having support from senior department and agency executives, such as the chief information officer (CIO), was critical to the success of the investments. For example, strong leadership support can result in benefits to a program, including providing the program manager with the resources necessary to make knowledge-based, disciplined decisions that increase the likelihood of their program's success. In addition, we have previously reported that an effective CIO can make a significant difference in building the institutional capacity needed to implement improvements to an agencies' information and technology management capabilities, which should result in technology solutions that improve program performance.²

To its credit, we recently reported that the Social Security Administration (SSA) had fully addressed in its policies, the role of the CIO with regard to leadership and accountability.³ 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.

Nevertheless, given its high turnover of CIOs, it will be important for SSA to ensure that the policies related to its CIO's responsibilities are clearly documented. As we reported in August 2018, the average tenure of SSA's CIO since 2004 has been 1.8 years. Our previous work has determined that a CIO should stay in office for 3 to 5 years to be effective and 5 to 7 years to fully implement major change initiatives in large public sector organizations.⁴

¹GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, GAO-12-7 (Washington, D.C.: Oct. 21, 2011).

²GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

³GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities*, GAO-18-93 (Washington, D.C.: Aug. 2, 2018).

⁴GAO-04-823.

2. What steps can the Social Security Administration take to make sure that long term IT investments stay on track when leadership changes?

In order for SSA to ensure that its long-term IT investments stay on track throughout leadership changes, the agency should take further steps to implement all of the requirements in federal laws and guidance that address the role of the CIO and document these roles in the agency's policies, as we recommended in our August 2018 report.⁵ While the agency had addressed the role of the CIO in the leadership and accountability area, as noted previously, it had not fully addressed the role of the CIO in five other policy areas that we examined.⁶

For example, SSA's policies minimally addressed the requirements for IT strategic planning. Specifically, while the policies required the CIO to establish goals for improving agency operations using 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. Further, the agency's policies did not address the IT workforce area (e.g., recruiting and retention) 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.

As a result, we recommended that SSA address the weaknesses in the five key policy areas. If SSA fully implements our recommendation, it should be better positioned to attract and retain high-quality leadership when there are vacancies, while also maintaining continuity of IT operations when leadership changes occur.

⁵GAO-18-93.

⁶These five policy areas are: IT strategic planning, IT workforce, IT budgeting, IT investment management, and information security.

KEVIN BRADY, TEXAS,
CHAIRMAN

SAM JOHNSON, TEXAS
DEWEN NUNES, CALIFORNIA
DAVID G. BERECHT, WASHINGTON
PETER J. ROSKAM, ILLINOIS
FERRI BLUMENFELDER, FLORIDA
ADRIAN SMITH, KANSAS
LYNN JENKINS, KANSAS
ERIK PAULSEN, MINNESOTA
KENNY MARCHANT, TEXAS
DANIS BLACK, TENNESSEE
TOM REED, NEW YORK
MIKE KELLY, PENNSYLVANIA
JIM RENACCI, OHIO
KRISTI NOEM, SOUTH DAKOTA
GEORGE HOLDING, NORTH CAROLINA
JASON SMITH, MISSOURI
TOM RICE, SOUTH CAROLINA
DAVID SCHWEIKERT, ARIZONA
JACKIE WALCHIRO, INDIANA
CARLOS CURBELO, FLORIDA
MIKE BISHOP, MICHIGAN
DARIN LAHROD, ILLINOIS
BRAD R. WENSTRUP, OHIO

GARY J. ANDRES,
STAFF DIRECTOR

Congress of the United States

U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS

1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625

Washington, DC 20515-6518

<http://waysandmeans.house.gov>

RICHARD E. NEAL, MASSACHUSETTS, RANKING MEMBER
SANDER M. LEVIN, MICHIGAN
JOHN LEWIS, GEORGIA
LLOYD DOUGGETT, TEXAS
MIKE THOMPSON, CALIFORNIA
JOHN B. LARSON, CONNECTICUT
FARR BLUMENFELDER, OREGON
RON KENDRICK, WISCONSIN
BILL PASCHKE, JR., NEW JERSEY
JOSEPH CHOWLEY, NEW YORK
DANNY K. DAVIS, ILLINOIS
LINDA SANCHEZ, CALIFORNIA
BRIAN HIGGINS, NEW YORK
TERRI BEWELL, ALABAMA
SUZAN DUBENE, WASHINGTON
JUDY CHU, CALIFORNIA

BRANDON CASEY,
MINORITY CHIEF OF STAFF

October 18, 2018

Rajive Mathur
Deputy Commissioner of Systems and Chief Information Officer
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Dear Mr. Mathur:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the September 27, 2018, hearing entitled "The State of Social Security's Information Technology." In order to complete the hearing record, we would appreciate your response to the following:

1. Congress passed the *Modernizing Government Technology (MGT) Act* as part of the *National Defense Authorization Act for Fiscal Year 2018* (P.L. 115-91) to provide agencies with new ways to fund technology modernization projects. Does the Social Security Administration (SSA) plan to use the authority provided in the MGT Act for its information technology (IT) modernization efforts? If not, why not?
2. In your testimony you noted that in most cases, even when the SSA identifies commercial software that can meet the agency's needs, the SSA needs to do significant development work to integrate that software into its systems. Will the SSA's IT modernization efforts make it easier to integrate commercial products into the SSA's systems?

Question from Rep. Mike Bishop

1. For decades, the SSA has relied on a stable and reliable mainframe infrastructure to support its IT systems needs, and the SSA's IT modernization plan released in October 2017 indicated that the SSA planned to continue to rely on mainframe technology for at least five more years. In your testimony, you stated that the SSA has moved from a cloud first to a cloud smart approach. How does the SSA plan to implement this strategy and what role does the SSA's current mainframe infrastructure play in this approach?

Questions from Rep. Carlos Curbelo

A new law requires your agency to modernize a service you provide to the financial industry, the Consent Based SSN Verification system (CBSV). This Committee unanimously passed legislation supporting this project.

1. What is your timeline for implementation of the new law?
2. The law gives the SSA the ability to upgrade existing resources or build a new system to meet the law's requirements. What approach is the agency taking, and why? How will this affect the cost of compliance?
3. As has been the history with the CBSV, users of the system have provided the funding to build and maintain it through user fees and enrollment fees. In keeping with this, the new law directs the SSA to collect half the implementation costs in advance from industry. What steps will you take to ensure that costs are reasonable for users?
4. The SSA is in the midst of a significant IT modernization effort. As you work through implementation, how will you ensure that any system design and funding requests will be used to successfully implement the law and not used to offset the agency's IT modernization costs?
5. In implementing the legislation, how do you plan to work with federal banking agencies, who are responsible for supervising and regulating the cybersecurity and privacy practices of financial institutions?

We would appreciate your response by **November 1, 2018**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to alex.stepahin@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,



Sam Johnson
Chairman
Subcommittee on Social Security



SOCIAL SECURITY

Office of Systems

November 15, 2018

The Honorable Sam Johnson
Chairman, Social Security Subcommittee
Committee on Ways and Means
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Thank you for the opportunity to provide information to complete the record from the September 27, 2018 hearing entitled "The State of Social Security's Information Technology." Enclosed please find our answers to your questions and the questions from Representative Bishop and Representative Curbelo.

I hope this information is helpful. If you have further questions, please do not hesitate to contact me or have your staff contact Royce Min, our Acting Deputy Commissioner for Legislation and Congressional Affairs, at (202) 358-6030.

Sincerely,

A handwritten signature in black ink that reads "Rajive Mathur".

Rajive Mathur
Deputy Commissioner for Systems
and Chief Information Officer

Enclosure

Post-Hearing Questions for the Record
Submitted to Rajive Mathur
Deputy Commissioner for Systems
Chief Information Officer
U.S. Social Security Administration

“The State of Social Security’s Information Technology.”
September 27, 2018

United States House of Representatives, Committee on Ways and Means,
Subcommittee on Social Security

QUESTIONS FROM CHAIRMAN JOHNSON

1. Congress passed the Modernizing Government Technology (MGT) Act as part of the National Defense Authorization Act for Fiscal year 2018 (P.L. 115-91) to provide agencies with new ways to fund technology modernization projects. Does the Social Security Administration (SSA) plan to use the authority provided in the MGT Act for its information technology (IT) modernization efforts? If not, why not?

Upon enactment of the MGT Act, we did a thorough assessment of which IT projects may be a good fit for either the Working Capital or Technology Modernization funds provided under the new law. Although we decided these new funding mechanisms were not a good fit for existing projects, they are certainly a potential source we can consider in the future. In the meantime, Congress appropriated the agency \$280 million in Fiscal Year (FY) 2018 and \$45 million for FY 2019 that is helping us accelerate implementation of our five-year roadmap for IT modernization (<https://www.ssa.gov/agency/materials/IT-Mod-Plan.pdf>).

2. In your testimony you noted that in most cases, even when the SSA identifies commercial software that can meet the agency’s needs, the SSA needs to do significant development work to integrate that software into its systems. Will the SSA’s IT modernization efforts make it easier to integrate commercial products into the SSA’s systems.

Yes, although we anticipate some level of customization would still be required for integration into our systems. Our IT modernization efforts will replace existing core systems with new systems built with a modern technology foundation that uses current system architectures, agile software development, automation, and cloud and shared services. The new systems will also have security and privacy functions built-in with modern security architecture and systems-wide security services. These changes will make it easier to acquire commercial products and services to meet our business needs.

QUESTION FROM REPRESENTATIVE MIKE BISHOP

- 1. For decades, the SSA has relied on a stable and reliable mainframe infrastructure to support its IT systems needs, and the SSA's IT modernization plan released in October 2017 indicated that the SSA planned to continue to rely on mainframe technology for at least five more years. In your testimony, you stated that the SSA has moved from a cloud first to a cloud smart approach. How does the SSA plan to implement this strategy and what role does the SSA's current mainframe infrastructure play in this approach?**

OMB recently released a draft Federal Cloud Computing "[Cloud Smart](#)" Strategy for public feedback. Once finalized, we will ensure that our approach follows the Federal guidance. Additionally, our business needs will continue to drive our cloud smart implementation, and we seek to leverage the right platform for the right business need. To that end, we expect to use the cloud for many existing and new enterprise applications where possible. Our hybrid cloud includes Amazon Web Service public cloud platform and an on-premise cloud. We will continue to use this combination as part of our overall cloud strategy.

Regarding our mainframe infrastructure, we will continue to optimize the mainframe platform to deliver high quality services and will use it in conjunction with our cloud efforts where it makes sense to do so, from a business, availability, and cost perspective. We expect to automate more of our mainframe infrastructure processes, as we are looking to incorporate additional tools for billing, cost support, and management oversight. In addition, we are automating workflows to increase efficiency in our processes to manage cloud resources.

QUESTIONS FROM REPRESENTATIVE CARLOS CURBELO

A new law requires your agency to modernize a service you provide to the financial industry, the Consent Based SSN Verification system (CBSV). This Committee unanimously passed legislation supporting this project.

- 1. What is your timeline for implementation of the new law?**

Our goal is to implement this law as quickly as possible. The timeline for development of the newly required system is dependent upon the collection of 50 percent of the associated start-up costs. Accordingly, we are working diligently on all fronts to finalize the new system requirements and costs so that we can begin collecting the applicable fees. As part of this process, we must engage the financial industry—the end users of this product—to make sure we understand its needs and how much it will use the system. We are also consulting with privacy experts and developing e-Signature requirements for electronic consent that will require updates to our regulations.

We will continue to keep the Subcommittee informed on our plans and actions to implement this law. We appreciate Congress' support to ensure that the costs for this non-programmatic workload are fully covered.

2. **The law gives the SSA the ability to upgrade existing resources or build a new system to meet the law's requirements. What approach is the agency taking, and why? How will this affect the cost of compliance?**

We are building a new, fully automated system, while using as much of our existing verification infrastructure as possible. It was not feasible to scale up our existing manual process, which currently supports about 80 users, to handle thousands of new users and a substantial increase in verification requests. We also need to build-in new oversight and monitoring features to meet related requirements in the law that will help ensure the security and integrity of the new system and processes. Most notably, our approach includes ongoing outreach with external stakeholders, and leverages the experience of subject matter experts from across our agency, to ensure we build an efficient, accountable, transparent, and secure process that meets the needs of the financial industry while preserving the privacy of our data.

Over time, we anticipate that the fully automated system will make it less expensive for us to enforce and maintain user compliance.

3. **As has been the history with the CBSV, users of the system have provided the funding to build and maintain it through user fees and enrollment fees. In keeping with this, the new law directs the SSA to collect half the implementation costs in advance from industry. What steps will you take to ensure that costs are reasonable for users?**

We are engaging the financial industry to determine the expected volume of users and transactions, which will allow us to determine all costs associated with building the new system. We will use this information to develop a fee structure that is proportionate to its use and equitable to users. We intend to leverage existing SSN verification infrastructure to the extent possible to reduce development costs.

We note that all applicable fees will be published in the Federal Register, allowing the public to comment on the fee structure to cover start-up and ongoing costs. Additionally, we plan to review established fees on a recurring basis, as we do now, to help ensure we recoup only the reasonable costs to cover our ongoing support and maintenance of this new verification system.

4. **The SSA is in the midst of a significant IT modernization effort. As you work through implementation, how will you ensure that any system design and funding requests will be used to successfully implement the law and not used to offset the agency's IT modernization costs?**

While the law provides that IT modernization funds can be used for developing this new system, we must be fully reimbursed to the extent these funds are used to implement this law. Executive level oversight and accountability will ensure that our IT funding is not offset and the users of this system cover all costs in full. Accordingly, we will closely monitor the accounting for this effort. We will use a separate tracking mechanism developed specifically to capture any funds expended throughout the agency for startup and implementation of this law. Our cost accounting system will capture all costs associated with this work and will be fully reimbursed by the users of the new electronic consent SSN verification system. We

will not include time spent on separate IT modernization efforts within these costs. Outreach suggests there will be strong participation from the financial sector, which will ensure necessary funding is available to cover all the costs associated with implementation of the law.

5. In implementing the legislation, how do you plan to work with federal banking agencies, who are responsible for supervising and regulating the cybersecurity and privacy practices of financial institutions?

To ensure data security and privacy compliance, we are engaging with the Big Tent Coalition (BTC) representing approximately 95 percent of financial institutions of permitted entities. We also received a detailed presentation on the regulations governing the various categories of the banking industry. The BTC is facilitating meetings for us with financial regulators from the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Federal Reserve Bank.

KEVIN BRADY, TEXAS,
CHAIRMAN

SAM JOHNSON, TEXAS
DUNCAN HUBBS, CALIFORNIA
DAVID G. REICHERT, WASHINGTON
PETER J. ROSKAM, ILLINOIS
VERN BUCHANAN, FLORIDA
ADRIAN SMITH, NEBRASKA
LYNN JENKINS, KANSAS
ERIK PAULSEN, MINNESOTA
KENNY MARCHANT, TEXAS
DIANE BLACK, TENNESSEE
TOM REED, NEW YORK
MIKE KELLY, PENNSYLVANIA
JIM RENACCI, OHIO
KRISTI NOEM, SOUTH DAKOTA
GEORGE HOLDING, NORTH CAROLINA
JASON SMITH, MISSOURI
TOM RICE, SOUTH CAROLINA
DAVID SCHWEIKERT, ARIZONA
JACQUE WALORSKI, INDIANA
CARLOS CUBELLO, FLORIDA
MIKE BISHOP, MICHIGAN
DAVIN LARSON, ILLINOIS
BRAD R. WENSTRUP, OHIO

GARY J. ANDRES,
STAFF DIRECTOR

Congress of the United States

U.S. House of Representatives

COMMITTEE ON WAYS AND MEANS

1102 LONGWORTH HOUSE OFFICE BUILDING
(202) 225-3625

Washington, DC 20515-6748

<http://waysandmeans.house.gov>

RICHARD E. NEAL, MASSACHUSETTS, RANKING MEMBER
SANDER M. LEVIN, MICHIGAN
JOHN LEWIS, GEORGIA
LLOYD DOGGETT, TEXAS
MIKE THOMPSON, CALIFORNIA
JOHN B. LARSON, CONNECTICUT
EARL BLUMENTHAL, CONNECTICUT
RON KARD, WISCONSIN
BILL PASCRELL, JR., NEW JERSEY
JOSEPH CROWLEY, NEW YORK
DANNY K. DAVIS, ILLINOIS
LINDA SANCHEZ, CALIFORNIA
ERIAN HIGGINS, NEW YORK
TERRI SEWELL, ALABAMA
SUZAN D. BENE, WASHINGTON
JUDY CHU, CALIFORNIA

BRANDON CASEY,
MINORITY CHIEF OF STAFF

October 18, 2018

Gale Stallworth Stone
Acting Inspector General
Office of the Inspector General
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Dear Ms. Stone:

Thank you for your testimony before the Committee on Ways and Means Subcommittee on Social Security at the September 27, 2018, hearing entitled "The State of Social Security's Information Technology." In order to complete the hearing record, I would appreciate your response to the following:

1. On September 24, 2018, an outage due to a computer error was reported of the Social Security Administration (SSA) Office of the Inspector General's (OIG's) online fraud-reporting form. What was the cause of the error, and has it been resolved?
2. What IT systems does the OIG use to carry out its core mission functions?
3. How does the OIG manage these core IT systems and when were these systems last updated?
4. What IT systems does the OIG use to process reports of fraud? When and how were these systems developed?

I would appreciate your response by **November 1, 2018**. Please send your response to the attention of Amy Shuart, Staff Director, Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 2018 Rayburn House Office Building, Washington, DC 20515. In addition to a hard copy, please submit an electronic copy of your response in Microsoft Word format to alex.stepahin@mail.house.gov.

Thank you for taking the time to answer these questions for the record. If you have any questions concerning this request, you may reach Amy at (202) 225-9263.

Sincerely,

A handwritten signature in black ink that reads "Sam Johnson". The signature is written in a cursive style with a large, prominent "S" at the beginning.

Sam Johnson
Chairman
Subcommittee on Social Security



November 1, 2018

The Honorable Sam Johnson
Chair, Subcommittee on
Social Security
Committee on Ways and Means
United States House of Representatives
Washington, DC 20515

Attention: Amy Stuart

Dear Mr. Chairman:

This is in response to your questions for the record, further to my testimony on September 27, 2018 before the Subcommittee on Social Security, Committee on Ways and Means, at a hearing on the state of the Social Security Administration's (SSA) information technology. I appreciate the opportunity to provide additional information to the Subcommittee. Below are responses to your specific questions.

1. On September 24, 2018, an outage due to a computer error was reported of the SSA Office of the Inspector General's (OIG) online fraud-reporting system. What was the cause of the error, and has it been resolved?

The OIG public fraud-reporting form is accessible from OIG's internet site, but it is housed on SSA's servers. On September 10, SSA made a change to a script that processes incoming allegations. The change was required to ensure compliance with enhanced IT security policies. The employee who made the change thought he or she was working in isolation on a test server and that the changes would not interfere with production. That was not the case; therefore, this change caused allegations received from 3:30 p.m., September 10 through 9:30 a.m., September 12 to be lost. After this incident, we met with responsible SSA staff to request updated documentation and to establish guidelines for future communication and testing procedures between SSA and OIG related to the public fraud-reporting form. SSA will notify OIG of any upcoming changes, and OIG personnel will test the process to ensure it is working prior to releasing the changes to production.

2. What IT systems does the OIG use to carry out its core mission functions?

The OIG Office of Investigations manages its workloads using the National Investigative Case Management System (NICMS), a Metastorm Business Process Management systems platform-based application using an Oracle database. The OIG Office of Audit manages audit work papers using TeamMate, a commercial off-the-shelf application. Although these are OIG applications, we use virtual servers hosted by SSA to house them, and our applications are subject to SSA's patches, updates, and security.

WEB: OIG.SSA.GOV | FACEBOOK: OIGSSA | TWITTER: @THESSAOIG | YOUTUBE: THESSAOIG

6401 SECURITY BOULEVARD | BALTIMORE, MD 21235-0001

Page 2—The Honorable Sam Johnson

3. How does the OIG manage these core IT systems and when were these systems last updated?

OIG IT staff manage NICMS, and we schedule updates/enhancements to the application quarterly, with occasional high-priority items implemented more frequently. We implemented the most recent updates to NICMS in October 2018. We implemented the most recent updates to OIG's Metastorm and Oracle applications in June 2017. TeamMate updates are implemented in conjunction with new versions released by the vendor (Wolters Kluwer). We completed the most recent OIG updates to OIG's production TeamMate version in February 2017. Testing of a new version of TeamMate is underway.

4. What IT systems does the OIG use to process reports of fraud? When and how were these systems developed?

There are four ways that reports of fraud are received and entered into NICMS for processing:

- Public citizens can submit reports of fraud using the public fraud-reporting form via the OIG internet site. The public fraud-reporting form was developed by SSA based on OIG's requirements in 2008. OIG most recently updated the form in August 2018.
- Individuals or entities can contact the OIG Fraud Hotline by phone, fax, or U.S. Mail. Fraud Hotline phone calls are answered at the National Center for Disaster Fraud, where staff uses the SSA OIG Hotline Complaint system to submit reports of fraud to OIG, and OIG staff then enter the reports into NICMS. The SSA OIG Hotline Complaint system is a Microsoft Dynamics-based application developed by Microsoft and implemented in November 2017.
- SSA employees can submit reports of fraud through the internal e8551 programmatic fraud referral form. SSA developed the e8551 form in 2002, and OIG has maintained it since 2011. OIG most recently updated the form in March 2018.
- Finally, designated OIG staff can directly enter reports of fraud into NICMS. NICMS was originally developed by OIG with vendor assistance (Booz Allen Hamilton) in 2004. OIG has updated and maintained the system since implementation, and is currently evaluating potential new applications/tools to support our mission.

Thank you for the opportunity to provide this information to help the Subcommittee carry out its oversight responsibilities. Should you have further questions, your staff may contact Walter Bayer, OIG Congressional and Intragovernmental Liaison, at (202) 358-6319.

Sincerely,


Gale Stallworth Stone
Acting Inspector General

[Submissions for the Record follow:]



Corporate Office
100 Kingsley Park Drive
Fort Mill, SC 29715
www.domtar.com

September 27th, 2018

Re: Statement Social Security Administration's Information Technology (IT), Including Modernization, Management and Acquisition

Dear Chairman Johnson:

Domtar appreciates the opportunity to comment on the Social Security Administration's state of Information Technology (IT) before the House Ways and Means Social Security Subcommittee. Domtar is a large producer of communication, specialty and packaging papers, market pulp and absorbent hygiene products. We are the market leader in North America in uncoated freesheet papers (UFS) employing nearly 10,000 men and women across the United States, Canada and Europe.

In 2011, the Social Security Administration ceased the mailing of earnings statements to all Americans, citing a need to modernize. After a backlash from a wide range of consumers, retirees, citizen's rights groups and others, statement mailings restarted in 2014 on a quinquennial basis until the wage earner reaches age 60, and on an annual basis from 60 until the time the person starts collecting their contributions.

There are two important factors that contributed to citizen's pushback on the agency's change. Social Security contribution statements are the single most important retirement planning tool a working American has at their disposal. Few young people may realize it at the time, but the importance of the information contained in the contribution statement cannot be overstated. Further, one third of Americans still lack access and/or technical know-how to receive electronic communications – a population segment that disproportionately skews towards seniors¹, lower-income individuals and rural populations² (2018 FCC Broadband Deployment Report and PEW Research Center - Technology Use among Senior).

Domtar applauds the Social Security Administration's desire to modernize as it is vital to keep our electronic infrastructure up-to-date. It is ironic that the SSA is embarking on a modernization drive, when it still falls short in meeting its most basic mission: providing vital tax information and documents to every US wage earner. These hearings and the actions of SSA presuppose that every wage earner has the proper IT assets and enough technological know-how to access forms, instructions and contribution statements. Such efforts overlook the plight of millions of Americans who are technologically disenfranchised.

I hope the Subcommittee will take note of these realities and make appropriate recommendations to the Social Security Administration.

¹ <http://www.pewinternet.org/2017/05/17/technology-use-among-seniors/>

² <https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2018-broadband-deployment-report>

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas Howard". The signature is written in a cursive style with a large, stylized initial 'T'.

Thomas Howard
Vice President, Government Relations



To the Members of the Subcommittee on Social Security:

There can be no doubt that SSA's online system is horrible. From my own personal vantage point, I've been attempting to order an online SS card replacement for weeks. Each time I attempt to access the system, I end up being blocked due to: 1) non-recognition of my password; and/ or 2) continuous looping of request for driver's license information. I called SSA to discuss, and was put on hold for over an hour (advised "wait time one hour, 15 minutes") -- unreasonable hold time under any circumstances (barring a national emergency). In the past, SSA provided an option to leave a name/telephone number for a call back (apparently to ease anxiety over excessive hold times), but in my experience this was never adhered to anyway and, as of my call today, is no longer presented as an option.

In conclusion, this Agency is impossible to deal with and its operations mirrored in secrecy and inaccessibility. Online or otherwise, completely user unfriendly, nearly impossible to get any assistance whatsoever. Am glad to see the Ways and Means Subcommittee is holding a hearing on the State of SSA's Information Technology. I posit that it is in total disarray and needs a major overhaul. With all the talk about "accessibility" and "governmental transparency," the SSA is an abject failure in relation to these critical public policy objectives. Not only is Congressional oversight necessary, the failures should be investigated by SSA's Inspector General for dereliction of duty and misapplication of public resources.

I am writing exclusively on my own personal behalf, though the issues presented are universal in scope.

Respectfully submitted:

Jacqueline Marie Merson
Attorney at law
5-24 49th Avenue, #4
Long Island City, NY 11101
718-614-6307
jmersonlaw@gmail.com





September 27, 2018

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
House Committee on Ways and Means
Washington, DC 20515

The Honorable John Larson
Ranking Member
Subcommittee on Social Security
House Committee on Ways and Means
Washington, DC 20515

Dear Chairman Johnson and Ranking Member Larson:

On behalf of the members of the Consumer First Coalition (CFC), I am pleased to submit this letter for the record for your Subcommittee hearing titled "Hearing on the State of Social Security's Information Technology."

CFC represents a group of leading financial services companies committed to combating new forms of fraud, protecting identities, and upholding the privacy protections that are a hallmark of the financial services industry. To meet these objectives and ensure consumer data and accounts are kept safe, the financial sector is constantly evolving and adapting to meet the dynamic challenges posed by sophisticated cyber criminals. Often, the best solution requires close collaboration among public and private stakeholders.

Such is the case with efforts to combat synthetic identity fraud, a particularly egregious form of identity theft that most often victimizes children. Earlier this year, your Committee unanimously passed legislation to address this type of fraud – the Protecting Children From Identity Theft Act, H.R. 5192, sponsored by Representatives Carlos Curbelo (R-FL), Kyrsten Sinema (D-AZ), Kenny Marchant (R-TX), and Randy Hultgren (R-IL) – and a similar version was signed into law as Section 215 of S. 2155, the Economic Growth, Regulatory Relief, and Consumer Protection Act. This new law directs the Social Security Administration (SSA) to modernize its system that provides the financial industry the ability to verify whether a given name, date-of-birth and Social Security number (SSN) match with what the SSA has on file. As part of a creditor's underwriting and fraud review of a new applicant, this piece of information can help prevent synthetic identities – which pair valid SSNs with fabricated personal information in order to create a "synthetic" credit history – from getting off the ground and harming the consumers whose SSNs were compromised.

Enacting this measure was a significant victory for consumers. Congress must now ensure implementation is a success as well. CFC and other industry stakeholders are actively engaged with

SSA in positive discussions to drive the implementation process forward. For example, while Congress specifically addressed the importance of privacy and data security for users of the SSA's verification system, it did not intend to deputize the SSA to regulate financial institutions. Those regulators already exist (e.g., Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System), and we are working with them to ensure that the legal protections afforded to the SSN itself are applied to SSA's confirmation of the SSN's validity. Financial institutions are regulated and examined for compliance to the highest standards of privacy and cybersecurity. We are hopeful the outcome will address the important concerns of Congress and the SSA, but not create duplicative compliance burdens for financial institutions.

Also, as you know, the new law gives the Commissioner of SSA broad latitude to set fees and determine costs for users of the system on both an ongoing basis to sustain the system, and to meet any system build or expansion demands placed on SSA by the new law. Without question, meeting the requirements of the law will result in significantly increased volume and a greater need for reliability and system up-time, which will require an investment by users of the system to achieve.

While the financial industry recognizes the importance of implementing a functional system that achieves Congress's goal of combating synthetic identity fraud, I would stress the importance to the Subcommittee of ensuring costs to users are not so high as to derail both the utility of the system and Congress's goal of protecting consumers from fraud. Modern technologies such as scalable system architecture and the increasingly common use of robust application programming interfaces (APIs) to facilitate real-time data exchange are just some of the methods and tools at SSA's disposal that can lead to a cost-effective yet highly sophisticated system that achieves all of Congress's goals.

In conclusion, thank you for holding this hearing today. While developing this verification system is just a small piece of the broader SSA IT modernization effort, it is one that has the potential to benefit millions of Americans – especially children – who might otherwise become victims of synthetic identity fraud. CFC is committed to working with SSA to successfully implement this new law by leveraging member firms' deep knowledge of privacy and data security compliance, as well as technological expertise that comes from building the most cutting-edge financial services platforms in the country.

Sincerely,

/s/

Jason Kratovil
Executive Director

