SOCIAL SECURITY ADMINISTRATION: INFORMATION SYSTEMS REVIEW

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 26, 2016

Serial No. 114–72

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

22–192 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
LIAM MCKENNA, *Senior Counsel*
SHARON CASEY, *Deputy Chief Clerk*

CONTENTS

SOCIAL SECURITY ADMINISTRATION: INFORMATION SYSTEMS REVIEW

Thursday, May 26, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 9:04 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Duncan, DeSantis, Blum, Hice, Carter, Grothman, Hurd, Palmer, Cummings, Connolly, Cartwright, Kelly, Lawrence, Watson Coleman, Plaskett, Welch, and Lujan Grisham.

Chairman CHAFFETZ. The Committee on Oversight and Government Reform will come to order.

Good morning. We are having an important hearing today on the Social Security Administration, Information Security Review.

During the past 2 years, this committee has heard a great deal about PII, personally identifiable information. Whether it is the Office of Personnel Management, the IRS, or the Department of Education, the Federal Government collects, maintains, transmits, and generates vast quantities of personally identifiable information.

The National Institute of Standards and Technology, otherwise known as NIST—whoops, I forgot to read this part.

Without objection, the chair is authorized to declare a recess at any time. My bad. Without objection, so ordered.

The National Institute of Standards and Technology, otherwise known as NIST, has said "unauthorized access, use, or disclosure of PII can seriously harm both individuals"—and they went on to say—"and reduce the public trust in organizations." NIST's assessment on the high value of PII to institutional credibility and personal privacy has been proven time and again perhaps no more poignantly than the data breach at OPM where tens of millions of Federal workers highly private, highly sensitive information on drug abuse, divorce, and even their fingerprints were taken by sophisticated attackers.

Ultimately, the cybersecurity battle is won as much in the boardroom as it is in the computer lab. Today's hearing will continue the committee's oversight on how Federal agencies are securing America's data, and this time we are talking to the Social Security Administration.

The information technology challenges Federal agencies face begin with the culture and leadership established by individuals such as those we have on the panel today. From the administrator

of the Social Security Administration to the chief information officer to the chief information security officer, the senior leadership has responsibility to modernize the Social Security Administration's technology and harden its information security posture to protect the massive amounts of PII traveling across the Social Security Administration's systems. And the volume of data is truly mind-boggling at this organization.

In short, the Social Security Administration stores the sensitive and personal identifiable information of virtually every American living and deceased. The Social Security Administration processes—and get these stats—processes an average daily volume of nearly 150 million transactions. In the past year alone, the data centers supported 1.6 billion automated Social Security number verifications; 251 million earnings items; 5 million retirement, survivor, and Medicare applications; 3 million initial disability claims; 1.5 million disability reviews; and 17 million new replacement Social Security card applications, a lot of work and a lot of good people working at the Social Security Administration.

This makes also the Social Security Administration a frontline target in the information age. Of concern is how that Social Security Administration networks bear the hallmarks of poor information security similar to those seen at OPM's networks back in 2014.

Year after year, penetration testers have been able to obtain global access privileges on the networks. This year, the agency didn't even detect the attack until auditors were told about them after sitting in the network for 3 days. The majority of Social Security Administration's 127 major application databases and 19.4 petabytes of data reside on mainframes which Social Security told testers they were "apprehensive about scanning or other rigorous testing because of its fragile operating posture." It is probably not a good sign when they don't want to do testing because they are afraid of how fragile the system is.

As has been proven by these pen tests or penetration tests, adversaries have been able to gain footholds into the networks, elevate privileges, and for the first time this year, do so completely undetected by the Social Security Administration, at least that we know of. Our cybersecurity conversation needs to move beyond firewalls and intrusion detection systems. Advanced persistent threats Federal agencies like Social Security face are adept at bypassing those sorts of perimeter defenses.

Moreover, the question is not whether adversaries are going to get inside the network but if they can be found before they do serious damage. And that conversation about the modern tools necessary to detect and mitigate advanced threat sectors is almost impossible to have when we can't get agencies like the Social Security Administration off of these legacy technologies.

We had an important hearing about this topic yesterday on the big broad problems and challenges that we face within the Federal Government, and here we are going to examine a specific agency, as we have done.

I would note that this committee has done something that has not been done before, and that is we have a subcommittee that is specific to the issues as it relates to information technology.

Social Security Administration has been using programming language such as COBOL and Fortran and ALC since the 1970s, over 66 million lines of that old code to support operating systems with the PII of all Americans. But I want to be fair. In spite of these facts, Social Security Administration is doing well in some areas, which gives me a sense of optimism for the security of my data, my children's data, and frankly, the data of everybody in this room.

In 3 out of the last 4 years the Social Security Administration scored at least 96 percent on the Office of Management and Budget's cybersecurity assessment, though the score for fiscal year 2015 dropped 12 percentage points to 84 percent. During the most recent penetration test of the Social Security Administration, the white-hat hackers were unable to gain access to Social Security's internal systems through public-facing systems. That is the good news. And Social Security Administration was able to improve their score on the most recent iteration of the FITARA scorecard from a D to a C.

There are some positive takeaways from here, but, however, in the world of cybersecurity it only takes one vulnerability, one port, one credential, or one back door to actually expose millions of people's information. This is one of the largest, most important organizations we have for the storage of data, and thus, we felt it was important to have this at the full committee hearing today.

Chairman CHAFFETZ. And with that, I will now recognize the ranking member, Mr. Cummings of Maryland, who I believe where the Social Security resides is in your district. So I will now recognize Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. And you are absolutely right. The Social Security Administration is located in the 7th Congressional District of Maryland. And of course it manages our nation's Social Security program, and certainly good to see the Honorable Carolyn Colvin, who I have known for many years, and I want to thank you for your leadership.

In fiscal year 2017, it will ensure that more than 50 million seniors and their dependents receive the benefits earned through their lifetime of work. That is about 89 percent of the United States population over the age of 65. To administer Social Security program, as well as the Disability Insurance program and the Supplemental Security Income program, the Social Security Administration collects sensitive data on nearly every American.

The data breach of the Office of Personnel Management affected more than 25 million people. A breach at the Social Security Administration could affect nearly every single person in this country.

The good news is that Social Security has never had a known exfiltration. However, threats are constantly evolving, and today's hearing will enable us to examine what more must be done to meet these threats and ensure that Social Security data remains safe and secure.

In many ways, Social Security's information technology systems are modeled for the Federal Government. The agency has saved about $370 million in its IT budget over 3 years. This sounds technical, but Social Security achieved highest individual metric grade for IT project savings on FITARA implementation scorecard metric

that our committee commissioned. In other words, it was the benchmark against which the other 23 agencies were measured.

However, Social Security is confronted by tens of millions of scans and probes every week trying to find vulnerabilities in the agency's defenses. Every second of every day determined hackers here in the United States and around the world are trying to breach Social Security's firewalls.

Audits of Social Security's IT systems and practices have found weaknesses that need to be corrected. In 2012, a FISMA audit reported that these shortcomings constituted a material weakness. The agency has worked to address these shortcomings, and more recent audits have found improvements in the agency's IT security.

But there is still "significant deficiency in internal controls" according to the most recent audit. Additional measures must be implemented to close remaining gaps. Unfortunately, Social Security's IT budget has been underfunded for years. According to the FISMA audit, one of the factors that contributed to the agency's significant deficiency was that "SSA focused its limited resources on high-risk weaknesses and therefore was unable to implement corrective action for all aspects of the prior year deficiencies."

And I hope that our witnesses will address this issue. At yesterday's hearing there was quite a bit of testimony with regard to whether there were sufficient funds going into these agencies to do the things that they needed to do. That argument goes back and forth, but we want to have a fair, accurate assessment of how the money is being used that you are getting, whether it is being used effectively and efficiently, and what difference would additional money make.

There are some in the Congress who believe that the more money you get—that you don't need any more money, and to be frank with you, I think all of us want to know exactly what the situation is. Are you asking to do more with less? I don't know, but I would like to know.

So Social Security benefits are funded through the Social Security tax paid by employers and employees. Funding for benefits is considered mandatory spending and is not subject to the appropriations process. However, the agency's administrative expenses are paid from the account that is funded by discretionary appropriations subject to the annual appropriations process. Congress's failure to adequately fund Social Security's administrative expenses has resulted in extended wait times for seniors calling the 800 number, reduced operating hours at field offices, and delays for adjudicative hearings that now average more than 500 days. Underfunding Social Security Administration has also affected its efforts to modernize its 40-year-old IT infrastructure and address evolving cyber risks.

The President's fiscal year 2017 budget seeks the first installment of what is expected to be a $300 million request over the coming years to upgrade Social Security's IT systems. Congress must act on this request and provide the agency the resources it needs to protect the data entrusted to it. Again, we want to know how those funds are going to be used if you get them and exactly whether they are being, again, used effectively and efficiently.

Shortchanging data security at Social Security as a senseless pursuit of austerity could put the privacy of every American at risk, and that is a risk we simply cannot afford to take.

And with that, Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I will hold the record open for 5 legislative days for any members who would like to submit a written statement.

I will now recognize our panel of witnesses. We are pleased to welcome the Honorable Carolyn Colvin, acting commissioner of the Social Security Administration; Mr. Robert Klopp, deputy commissioner of systems and chief information officer at the Social Security Administration; Ms. Marti Eckert, associate commissioner of information security and chief information security officer at the Social Security Administration; and Ms. Gale Stallworth Stone, deputy inspector general at the Social Security Administration. We thank you all for being here.

Pursuant to committee rules, all witnesses are to be sworn before they testify, so if you will please rise and raise your right hand.

[Witnesses sworn.]

Chairman CHAFFETZ. Thank you. If you will please be seated and let the record reflect that the witnesses all answered in the affirmative.

In order to allow time for discussion, we would appreciate it if you would limit your comments to 5 minutes. Your entire written statement will be entered into the record.

So we are pleased again to have the acting commissioner here, Ms. Colvin, and you are now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF CAROLYN W. COLVIN

Ms. COLVIN. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for inviting us to discuss IT at Social Security. My name is Carolyn Colvin, and I'm the acting commissioner of the Social Security Administration.

Just to provide you of the scope of what we do at SSA, with an appropriation of around $12 billion in 2015, we paid more than $930 billion in benefits to nearly 67 million people that year. In addition, we maintained earning records for nearly every American and completed over 8 million claims for benefits. My written testimony provides further examples. Our IT infrastructure supports all of this work.

I'm pleased to be here, along with our chief information officer Robert Klopp and our chief information security officer Marti Eckert. Mr. Klopp has impressive private industry expertise in leading technology change and in balancing that change with reliable service delivery. And Ms. Eckert is an excellent public servant who has done great work to strengthen our cybersecurity program.

The security and integrity of our IT systems is of paramount importance to me, and I value Mr. Klopp and Ms. Eckert's advice and guidance. I and other agency leaders communicate with them regularly to discuss IT and cybersecurity issues.

Today, I will describe in brief how IT supports our mission and the need for a multiyear IT modernization effort. Mr. Klopp will

discuss how we invest in and manage IT and our paths and achievements in modernizing our IT infrastructure. Ms. Eckert will summarize our continuous cybersecurity efforts and improvements.

We are all committed to working with Congress and OMB to invest our IT dollars wisely, improve our cybersecurity, and ensure compliance with FISMA and FITARA. Investing wisely in technology is one of my priorities as we work to deliver smart, secure, and efficient service. We must use all of our IT funding for ongoing operational costs such as our network of field offices, national 800 number, and our online services.

Each year, we see greater numbers of people across all demographics doing business with us online. Since we launched My Social Security in 2012, over 24.5 million customers have created accounts. In fiscal year 2015 we received more than half of all Social Security retirement and disability applications online, including 75 percent of Medicare applications.

That said, we have a significantly aged IT infrastructure which is increasingly difficult and expensive to maintain. Although our legacy infrastructure is not sustainable over the long term, these aged systems are the very tools that we rely upon each day to provide service to the public. We must maintain these legacy systems while developing their replacements.

Let me be clear. We need a sustained, long-term investment to make the changes needed to develop a fully modern IT infrastructure that is capable of supporting the millions of people we serve every day, not to mention workloads that are growing as the baby boomers age. That is why the President's budget for 2017 requests a multiyear mandatory funding stream so that we can undertake IT modernization that will bring our systems up to modern standards.

As we continue to provide opportunities for better customer service through new online services, we must remain vigilant in continuing to strengthen our cybersecurity. I am firmly committed to protecting the public's information. Our cybersecurity defense capabilities are comprehensive, multilayered, and strong. They safeguard the public's information against evolving threats and cyber attacks. We have a rigorous approach to cybersecurity testing, and we try to hack our own systems every day. We also work with independent auditors and Homeland Security. We are continually strengthening our defenses.

In conclusion, we must position our agency for future success, and this must involve smart IT investments and a nimble cybersecurity program. I've worked to assemble a first-rate systems team at Social Security, and I fully expect that we will meet the challenges before us. With sustained and adequate funding, we will continue to provide the high-quality services the public expects and deserves.

I thank the committee for your support, and I will be happy to answer your questions.

[Prepared statement of Ms. Colvin follows:]

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting us to discuss information technology (IT) and security at the Social Security Administration (SSA), including our agency's compliance with the Federal Information Security Management Act (FISMA) and the Committee's scorecard on the Federal Information Technology Acquisition Reform Act (FITARA).

I will focus my testimony on providing an overview of the programs that we administer, describing in brief how IT supports our mission, our IT investment process, cybersecurity, and the need for a multi-year IT modernization effort. Mr. Klopp, our Deputy Commissioner for Systems and Chief Information Officer, will discuss how we invest in and manage IT, consistent with the principles of FITARA, and our plans to modernize our IT infrastructure. Ms. Marti Eckert, our Chief Information Security Officer, will summarize our cybersecurity efforts, and our compliance with FISMA.

At the outset, let me emphasize that investing wisely in technology is one of our top critical priorities as we work to deliver smarter, secure, and more efficient service. We have consistently used our IT resources to help us efficiently and effectively deliver benefit payments and other services to millions of Americans each year. Yet we have major challenges before us. We have a significantly aged IT infrastructure, which is increasingly difficult and expensive to maintain. In addition, we must dedicate substantial resources to ensuring the security and integrity of our IT systems and the vital data that we maintain. While I am confident in the abilities of our employees to handle these challenges, I must emphasize that we need a multi-year investment to make essential improvements to modernize our systems.

Overview of SSA

I would like to describe briefly the programs that we administer. Old-Age, Survivors, and Disability Insurance (OASDI) (or "Social Security") is a social insurance program, under which workers earn coverage for retirement, survivors, and disability benefits by working and paying Social Security taxes on their earnings.

We also administer the Supplemental Security Income (SSI) program, which provides monthly payments to people with limited income and resources who are aged, blind, or disabled. Adults and children under the age of 18 can receive payments based on disability or blindness. General tax revenues fund the SSI program.

Few government agencies touch as many people as we do. Social Security pays monthly benefits to more than 59 million individuals, consisting of 39 million retired workers and 3 million of their spouses and children; 9 million workers with disabilities and 2 million dependents; and 6 million surviving widows, children, and other dependents of deceased workers. We provide SSI benefits to over 8 million recipients.

The scope of our work is immense. In FY 2015, we:

- Handled approximately 37 million calls on our National 800 Number;
- Served about 40 million visitors in our 1,200 field offices nationwide;

- Completed over 8 million claims for benefits and more than 660,000 hearing dispositions;
- Handled over 35 million changes to beneficiary records;
- Issued about 16 million new and replacement Social Security cards;
- Performed almost 2 billion automated Social Security number verifications;
- Posted about 266 million wage reports;
- Handled over 18,000 cases in Federal District Courts;
- Completed over 2.2 million SSI non-medical redeterminations;
- Completed 799,000 full medical CDRs; and
- Completed approximately 3 million overpayment actions.

We handle all of this work with considerable efficiency. At approximately 1.3 percent of our total outlays, SSA's administrative expenses continue to be a small fraction of overall program spending, demonstrating the agency's cost-conscious approach to managing its resources.

The Role of IT at SSA

IT plays a critical role in our day-to-day operations. We use most of our IT funding for ongoing operational costs such as our National 800 Number service and our online services, both of which help us keep pace with the recent increases in claims. In FY 2015, our IT infrastructure supported the payment of more than $930 billion in benefits to nearly 67 million people and the maintenance of hundreds of millions of Social Security numbers and related earnings records for nearly every American.

We are exploring and developing ways we can expand our online customer base. Each year, we see greater numbers of people across all demographic segments doing business with us online. Since we launched *my* Social Security in 2012, over 24.5 million customers have created accounts. In FY 2015, customers continued to increase their use of our online services to conduct business with us as they completed over 87 million transactions via our website. In FY 2015, we received more than half of all Social Security retirement and disability applications online, including 75 percent of Medicare applications.

Customer satisfaction with our online services also continues to shine, as five of the top ten ranked Federal websites were SSA online customer service products, according to the 2015 ForeSee e-Government Report Card. We will continue to enhance our online services and promote them as a safe and convenient service option to increase usage and reduce unnecessary field office visits. Our goal is to increase the volume of online transactions by 25 million each year, which would result in 112 million transactions in FY 2016 and 137 million in FY 2017. With increased usage of online services, we can free up more time for customers that need or prefer to complete business with us in person.

We continue to increase the services available on our online *my* Social Security portal. Individuals may access their Social Security Statement at any time through their personal online *my* Social Security account. In 2015, we added several new services to our *my* Social Security portal including replacement Medicare Card services, and the capability for *my* Social Security users to download data from their Social Security Statement to assist them in financial and

retirement planning. Other online service efforts include a successful limited rollout – up to eight States and the District of Columbia over the last year– of a secure Internet Social Security Number Replacement Card application for eligible U.S. citizens age 18 and over. We expect to expand this service to other States in the near future.

In this calendar year, we are enhancing our online *my* Social Security service so that it is more compatible with mobile devices to improve service to that fast-growing segment of the user community. In addition, we are developing new customer engagement tools including Click-to-Chat and a Message Center for relaying informational messages to *my* Social Security users. Other services include the development of a Smart Claim application that will allow our customers to get a detailed status on their benefit applications within *my* Social Security. We will later expand Smart Claim to include online service options for SSI claimants as well.

IT Investment

While we have always been an efficient organization, with low administrative expenses, I fully appreciate that SSA must continually strive to improve how it invests resources, particularly in IT. Consequently, transforming the information technology investment process has been one of my highest priorities as Acting Commissioner. Over the last year, we have developed an IT Investment Process (ITIP) that will improve the way we manage and invest in IT at SSA.

Consistent with FITARA, ITIP will focus on up-front project planning with outcomes tied to specific agency goals. Improved project planning and documentation will allow us to assess project costs and timelines with greater accuracy. In addition, an enterprise-wide executive IT investment board will meet throughout the year to make informed funding decisions on projects that provide the greatest benefit to our agency's mission. As a result, we will be better able to deliver the right project on time and within budget, and provide the best tools for our employees and superior service to the American public.

In addition to improving how we invest in IT, we also are taking steps to ensure that we are recruiting the best talent and exploring the latest methods in the world of IT. To that end, last year I selected Rob Klopp to serve as our Deputy Commissioner of Systems and our Chief Information Officer. Mr. Klopp has impressive private industry expertise in leading technology change and balancing that change with reliable service delivery. In addition, we are working to build a digital services team that will bring private sector best practices into the disciplines of design, software engineering, and product management to maximize the agency's most important services. Finally, we are using new methods to deliver technology faster, such as Agile development and cloud computing services.

Cybersecurity

Our cybersecurity program continues to increase our detection, protection, and intelligence capabilities for strengthening the agency's defenses against evolving threats and cyber-attacks. Our program incorporates these security capabilities into a comprehensive, multi-layered defensive approach for ensuring the confidentiality, integrity, and availability of the public's sensitive personally identifiable information. As we continue to provide new opportunities for

better customer service through new online services, we must remain vigilant in continuing to strengthen our cybersecurity program capabilities.

To that end, we proactively try to penetrate our own information systems every day. With ongoing analysis and rigorous testing, we continuously learn more about the ways hackers may try to gain access to our systems, and we continuously devise ways to stop them.

Our cybersecurity program compares well against other Federal departments and agencies in key performance standards. To remain strong, we need to continue to evolve our cybersecurity program to reflect changes in technology, changes to business processes, and changes in the complexity of internal or external threats. Continued investments in cybersecurity projects and initiatives will ensure we have the resources needed to accomplish our agency's mission and thus maintain public confidence in the agency's ability to protect their privacy. Marti Eckert, our Chief Information Security Officer, will describe in more detail the steps we take to ensure the security of our information systems.

Additionally, to protect citizens' personally identifiable information further, we continue to improve authentication for our online services. In compliance with Executive Order 13681 ("Improving the Security of Consumer Financial Transactions"), we are changing our current multifactor authentication process for *my* Social Security from optional to mandatory for all users. Upon implementation this summer, all customers must enter a username, password, and a one-time passcode texted to a registered cell phone in order to access their *my* Social Security account. In the future, we expect to offer additional multi-factor options, pursuant to Federal guidelines. The National Institute of Standards of Technology is working on a revised guideline, and we are providing input into that process.

IT Modernization

I appreciate the Committee's interest in our efforts to modernize our legacy information systems. The database systems our agency uses today are 40 years old and are no longer the best solution to administer our programs. For several years, we worked to modernize our IT in small pieces at a time, but we have exhausted nearly all of these small efforts. The legacy infrastructure is not sustainable, but these aged systems are the very production tools that our employees rely upon each day to provide service to the public. We must maintain the legacy systems while, in parallel, developing their replacements. We are now at a point where we must undertake a larger, multiyear effort.

A portion of the fiscal year 2016 appropriation helps to begin the design of the legacy replacement systems. However, we need a sustained, long-term investment to make the changes needed to develop a fully modern IT infrastructure that is capable of supporting the immense responsibilities I described earlier in my testimony. That is why the President's Budget for FY 2017 requests multiyear funding of $300 million spread over four years, to undertake an IT modernization project that will bring our systems current. In FY 2017, $60 million is included as part of the FY 2017 President's Budget. The FY 2017 President's Budget also contains a mandatory proposal for additional IT modernization funding - $80 million each year in FYs 2018-2020. The project will require effort and investment in several areas including

modernization in computer language, database, and infrastructure. Mr. Klopp will describe in greater detail why such a long-term investment is essential.

Conclusion

Thank you for holding this important hearing. I am glad to highlight for you the importance of IT in our administration of the Social Security and SSI programs, and the need to ensure the integrity of our systems and the development of a sound IT investment process. I would be happy to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

Mr. Klopp, you are now recognized for 5 minutes.

STATEMENT OF ROBERT KLOPP

Mr. KLOPP. Chairman Chaffetz, Ranking Member Cummings, and members of the committee.

Chairman CHAFFETZ. Sorry, if you just move that mic a little bit closer right up there. There we go. Thank you.

Mr. KLOPP. Okay, cool. Thank you for inviting me to discuss IT at Social Security. My name is Rob Klopp, and 2015 Acting Commissioner Colvin appointed me to serve as SSA's deputy commissioner for systems and chief information officer. Prior to my appointment, I worked for a variety of private sector technology firms based in the Silicon Valley and elsewhere on the West Coast. I was recruited by the U.S. Digital Service's staff to try to help.

It was clear from the first day that the challenge facing the SSA comes from an aging IT infrastructure serviced by an aging IT staff. With acting Commissioner Colvin's full support and leadership, here is what we've accomplished in the last 17 months. We've started modernizing the underlying infrastructure and now have an authorization to operate production systems from the cloud. We have started modernizing our data architecture and will have a modern citizen database in production by the end of this calendar year. With this deployment, we will decommission our enumerations master file that has served us for over 30 years.

We've deployed a modern development environment that provides a basis for all new software development within the agency. This continuous development infrastructure will help us to significantly reduce the cost of developing, testing, and deploying modern software and will provide the basis for DevOps, the "new" new thing in software engineering.

We have developed an enterprise data warehouse that will provide the agency with an integrated view of current and historical data across every aspect of the agency. This warehouse will provide the foundation upon which the SSA may become a data-driven enterprise.

We have deployed significant new cybersecurity defenses and are beginning the deployment of yet another.

We have reorganized our systems staff to get more focus on cybersecurity, on software engineering, and on servicing our business components. As part of this, we have started hiring the next generation of IT staff and have procured a state-of-the-art 90-day coding boot camp to create our own digital services organization. This boot camp and the other organizational changes are designed to make us more agile from the top to the bottom.

Further, we are organizing around products instead of around projects. This is a critical new approach that will help us to minimize the effort that we now call maintenance and reduce the accumulation of technical debt. It is technical debt that forces us to spend millions on IT modernization. This topic of product management is one that I hope you will ask me about later.

We have developed a new IT investment process to help us start product development off the right foot and allow us to better track the actual benefits we estimated in our early cost-benefit analysis.

We have started the first very modern product development, DCPS. This Disability Case Processing System product will deliver the long-promised and much-needed capabilities to assist in disability determination. DCPS is modern through and through using state-of-the-art programming languages, open-source software, and the cloud. Development of the first release is completely agile, and the customers will see the work progress after each 2-week sprint. This first release is hitting development milestones on time and on budget, and we are optimistic that deployment for the first three States will begin this calendar year.

Finally, we have engaged the agency and challenged them to rethink how we engage our customers. Our customer connect product is very ambitious, and it will set the stage for modern IT by providing a perspective of what systems must look like 5 years from now when applications like Uber are passe.

It's been an amazing year. These are not initiatives just on the books. They are in flight and will deliver operational code this year. But there are issues. My biggest concern is around sustained funding. With the support of the acting commissioner, we've made great strides, but the foundation for modernization effort is all that we've built. We can modernize the agency, but we will require extra funding to keep the legacy systems running and keep servicing the public. The SSA delivers checks that represent 5 percent of the U.S. GDP, and that is not an insignificant operation.

If we try to modernize in small increments, we will progress at a pace that is slower than the pace of technology that technology advances and actually lose ground. I think the time to rebuild is now while the legacy systems are still supported by the staff who developed it.

Rebuilding aged IT infrastructure is not unlike rebuilding other aging infrastructure. Roads, bridges, dams, and/or the grid requires an investment and a strong effort. We look forward to working with Congress to overcome these challenges. Thank you, and I look forward to your questions.

[Prepared statement of Mr. Klopp follows:]

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me to discuss information technology at the Social Security Administration (SSA), including our agency's compliance with the Federal Information Security Management Act (FISMA) and implementation of the Federal Information Technology Acquisition Reform Act (FITARA).

In 2015, I was appointed to serve as SSA's Chief Technology Officer. Acting Commissioner Colvin subsequently appointed me to serve as SSA's Deputy Commissioner for Systems and Chief Information Officer. Prior to my appointment, I worked for a variety of technology firms based on the West Coast and in the Silicon Valley. I learned quickly that SSA has a committed and qualified IT workforce that maintains several significant information systems to meet its mission. To provide one measure of this, during fiscal year (FY) 2015, the agency paid more than $930 billion to almost 67 million beneficiaries representing around five percent of the U.S. Gross Domestic Product. The Acting Commissioner's written testimony provides an overview of how our IT supports our administration of the Social Security and Supplemental Security Income (SSI) programs. To support these payments, and the substantial other work that our agency performs, our total IT expenditure, in FY 2015, including our staff and contractors, was about $1.8 billion.

The SSA faces several IT challenges in the years ahead. The systems that serve our mission are old and they are primarily supported by the staff who developed them 30+ years ago. As this staff retires, the knowledge of these old applications and the knowledge of the legacy infrastructure they are built upon will diminish. We have to modernize these legacy systems before this knowledge is gone. Developing the new capabilities based on new technology to best serve the public is an expensive proposition if we have to build it upon this aging foundation. We have to modernize these legacy systems to provide these new services at a reasonable cost. In addition, we face threats to the security of the information we store at the Agency. Dealing with these threats requires constant vigilance. We need to modernize our legacy systems to provide the modern infrastructure that incorporates modern cyber defenses. (Ms. Eckert's testimony describes further our cybersecurity posture and our compliance with FISMA.) Below, I will detail some of the efforts we are making to improve how we invest in IT and our efforts to modernize our IT infrastructure. However, we need adequate and sustained funding from Congress to ensure that we can address these efforts over the long-term.

Implementation of FITARA and IT Investment

Many of our IT modernization and other practices align with the recently passed Federal Information Technology Acquisition and Reform Act, better known as FITARA. FITARA reforms aim to increase Federal CIO authority for IT planning and decision making, enhance management of Federal IT investments, and improve acquisition of IT human capital, products, and services.

We are fully engaged with our responsibilities pursuant to FITARA and the Office of Management and Budget (OMB) guidance to implement the law. We are making enterprise level improvements to important components of our Capital Planning and Investment Control

(CPIC) framework including: incorporating new policies and procedures for our IT investment review process; implementing a new integrated CPIC tool to replace a number of dated systems; and reorganizing several IT governance groups into a single, coordinated component.

FITARA and OMB guidance require agency CIOs to provide OMB on a regular basis information about major IT investments, including rating such investments according to risk. OMB reviewed our evaluations on our IT investments and found us in compliance with its guidance. We continue to revisit our process and rating criteria and our source documentation for improvement opportunities.

I am pleased to report that, over the last year, we developed a new IT Investment Process (ITIP) that will improve the way we manage and invest in IT at SSA. ITIP will focus on up-front project planning with outcomes tied to specific agency goals. Improved project planning and documentation will allow us to assess project costs, risks, and timelines with greater accuracy. In addition, an enterprise-wide executive IT investment board will meet throughout the year to make informed funding decisions on projects that provide the greatest benefit to our agency's mission. As a result, we will be better able to deliver the right project on time and within budget, and provide the best tools for our employees and superior service to the American public. Finally, the new process will include formal post-implementation reviews that look at the IT implementation process and at the ongoing return-on-investment, planned and actual, of the resulting business applications.

IT Modernization

In the late 1970s and early 1980s, because of the massive scale of our operations, SSA was aggressively developing systems and databases to store information about tens of millions of citizens. These systems were leading edge systems that pushed the state of the art in the 1980s.

Today, these legacy systems are out-of-date, and the cost required to bring them to a modern state represents a technical debt that accrues interest with each passing year. Their complexity makes it costly and challenging to add the functionality needed to meet the continually evolving requirements placed on us by the Administration, Congress and the people we serve. The extra cost of building on these aging systems represents part of this technical debt. Our university systems generally are no longer teaching the mainframe computer application languages, development, and operating environment, and the Federal staffs who developed and maintained these systems are retiring. As a result, the interest payments on this 30-year-old technical debt are compounding, and in the next five years, we could face a crisis keeping our systems running.

Generally, our approach to modernizing our major IT systems has been to replace components of systems rather than the system as a whole. This approach tends to reduce risk by reducing interdependencies in a single development effort and by reducing the scope of the modernization effort.

For several years, we have chipped away at the legacy code base as we add new business functionality, reducing our technical debt. This incremental and opportunistic approach worked well given the ebb and flow of annual funding. However, we are at a point where this approach

is no longer viable; technology is advancing faster than we can incrementally modernize. As a result, we have to undertake larger, multiyear tasks. To that end, we are focusing our efforts in three primary broad areas: database modernization, code modernization, and infrastructure modernization.

Our first broad area of focus is core database systems. Because of limitations in the technology available when our databases were designed, all updates were managed via a sequential, batch process that applied updates queued during the day. Modern databases update in real time. In addition, legacy databases were designed around specific applications rather than organized around data subjects. This creation of data silos makes adding broad agency-wide capabilities difficult and expensive. In the last year, we have started to re-organize our data into a modern architecture and began development of a framework to allow real-time updates. Unfortunately, all the legacy code base that we have becomes the issue.

Therefore, our second broad area of focus is modernizing that legacy code. Our efforts here are designed to address the complexity and pre-modern design of our oldest systems. We are exploring ways to capture value from the legacy code base, either through a code migration or by capturing the "gist" of the business rules. We are exploring different options, including "buy" as opposed to "build." We are also aggressively moving to modernize our software engineering tools and skills. In order to modernize the skill of our staff, with the aim of reducing the costs of modernization, we will develop an intensive training program. We have one very significant new project where we are using these skills to develop a brand new system and, so far, the impact is very positive. Finally, we are fully embracing agile development methods. This approach enables us to roll out more quickly new functionality to users while reducing the risk that what we produce will not meet users' needs.

The third broad area of focus is modernization of our infrastructure. For more than 30 years, we have been predominantly a user of mainframes for our mission-critical systems. For many years, only mainframes could handle our workload. In response to Acting Commissioner Colvin's direction to push us towards becoming a more data driven enterprise, we are deploying a modern business intelligence eco-system in the cloud. We are working to develop an on premises cloud environment and then a hybrid cloud environment to further enable us to take advantage of the economics of cloud computing. We have also established a Modern Development Environment (MDE) in the Amazon Web Services cloud. MDE is a suite of tools and engineering practices for supporting modern software development.

With our plan to leverage our new data capabilities, development techniques, and infrastructure, we are beginning a fundamental review of how we engage our customers and our employees. Through a new "Customer Connect" initiative, we are considering how better to meet customers experience in 2020. This initiative aims to reconsider not just our technology infrastructure, but to challenge SSA to reassess the business processes that have grown and evolved over the last eighty years.

Conclusion

Before we turn to cybersecurity, I would like to restate the core challenge I see.

As we head into this period where a significant portion of our IT staff becomes eligible for retirement, we need to begin long-term efforts to modernize our infrastructure, our data architecture, and our software intellectual property. We need to accomplish this while we keep the current systems incrementally advancing and while we continue to expand our commitment to cybersecurity.

Because our efforts have to be long-term, we need a stable long-term commitment to fund IT modernization, as discussed in the Acting Commissioner's testimony. We need funds to enable the modernization in the same way the nation needs funds to modernize other aging infrastructure, such as roads, dams, and the grid.

We look forward to working with Congress to overcome these challenges. Thank you and I would be glad to take any questions.

Chairman CHAFFETZ. Thank you.

Ms. Eckert, you are now recognized for 5 minutes.

STATEMENT OF MARTI A. ECKERT

Ms. ECKERT. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for inviting me to discuss information security at the Social Security Administration. My name is Marti Eckert, and I am the agency's chief information security officer. In this role I support our CIO and our agency's commitment to protect the information we manage and our systems from threats and vulnerabilities.

Today, I will briefly discuss our cybersecurity program and some of the measures we are taking to counter potential cyber threats.

We take seriously our responsibility to protect the information the public provides us. We take a strong, proactive approach to risk assessment and mitigation associated with securing this information in our many systems. We have strong controls in place, but we know that in today's escalating threat environment there is no perfect way to lock down every system. Every cybersecurity program must be a practice of continuous improvement.

We employ a dynamic enterprise-wide cybersecurity program and leverage a defense in-depth strategy to help protect our network, our data, and our employees. We work to protect our information, detect attacks, identify suspicious activities and systematically respond to software and hardware vulnerabilities. We use an integrated proactive defense strategy that enables us to carry out the agency's mission and meet customer expectations in a safe and secure environment.

To keep our information safe, we use a comprehensive holistic approach comprised of many technology solutions, policies, and awareness programs. Our cybersecurity program meets or exceeds all federally established oversight goals, and as technology and standards evolve, we continue to meet newly established benchmarks and security requirements each year. We addressed the NIST cybersecurity framework core functions of identify, protect, detect, respond, and recover.

To ensure we have a strong and robust program, we also collaborate with other Federal agencies such as Homeland Security to address cyber threats. We have no critical vulnerabilities, as identified on DHS's Federal Cyber Exposure Scorecard, and we meet all nine of the cross agency priority cybersecurity goals on information security defenses.

We are proud of our cybersecurity program but remain vigilant and continually improve and mature our defenses. We have developed several cybersecurity best practices that we share with other Federal agencies.

We continue to build upon the work we did last year during the Cybersecurity Sprint to put in place standard practices such as multifactor authentication. Since fiscal year 2012 we have offered a multifactor identification method for citizens to conduct business with us online on our My Social Security portal. This summer, we will make multifactor authentication mandatory for My SSA users in compliance with the Cybersecurity Act of 2015 and Federal directives.

We rank sixth in our peer group of 24 CFO Act agencies when it comes to FISMA compliance. In fiscal year 2015 our overall score was lower than the previous year due in part to a change in scoring metrics. Most of our reduced compliance metrics fell into the area of risk management.

Let me assure you we take the auditor's findings seriously, and we have completed actions on many recommendations from the FISMA assessment. For example, we implemented a zero-tolerance policy and immediate remediation for weak credentials. We prioritize our actions when remediating audit findings to address the most significant risks first following best practices and making best use of limited resources to address open recommendations.

To sustain a robust information security program, we must respond with newer and innovative defenses that will improve our ability to react quickly. Our plans include the use of more analytics tools to identify threats faster and the use of automation to respond and remediate incidents more quickly, as well as updating technology to reduce our reliance on outdated processes.

Your support in providing sustained adequate funding is critical to ensure we maintain and evolve the high level of information security the public expects and deserves. Thank you, and I will be happy to answer any questions.

[Prepared statement of Ms. Eckert follows:]

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for inviting me to discuss information security at the Social Security Administration (SSA), including our agency's compliance with the Federal Information Security Management Act (FISMA) and the Committee's scorecard on the Federal Information Technology Acquisition Reform Act. As the agency's Chief Information Security Officer, I support our Chief Information Officer in our agency's commitment to protect the information we manage and our systems from threats and vulnerabilities.

The security of the personally identifiable information (PII) the agency holds is of the utmost importance, and we take seriously our responsibility to protect the information provided to us by the public we serve. The agency has a strong, proactive approach to the identification and mitigation of risks associated with our online authentication to access public services via the internet, external and internal access to our secure network, and our information and communications assets. While we have strong controls in place, we know that there is no perfect way to lock down any system. In today's escalating threat environment, every cybersecurity program is a practice of continuous improvement.

Consequently, we continually work to keep pace with advancements in cybersecurity technology. We strengthen our security by remediating gaps in our security posture and institutionalizing and maturing security processes. We take a risk-based approach and leverage current agency processes, as we add layers of defense to improve protections and identify threats. Below, I will discuss in brief our cybersecurity program and some of the measures we are taking to counter potential cyber threats. Given the sensitive nature of this issue, I am unable to provide a detailed description of our cybersecurity capabilities in a public forum. However, I would be pleased to offer to you and your Committee staff a confidential briefing on this important issue.

Defense in Depth Strategy

At SSA, we employ a dynamic enterprise-wide cybersecurity program leveraging a defense-in-depth strategy to help protect our network, data, and employees while enabling the Agency's mission and meeting customer expectations in a safe and secure environment. We work diligently to protect our information, detect attacks, identify suspicious activities, and systematically respond to software and hardware vulnerabilities. We collaborate with the Department of Homeland Security's (DHS) United States Computer Emergency Response Team (US-CERT), the White House National Security staff, the Federal Chief Information Officer, and various law enforcement agencies to address cyber threats. We realize that technical solutions alone cannot combat adversarial threats in today's threat landscape, and it is not a single technology or process that keeps Social Security information safe, but rather an integrated, holistic approach comprised of many different technologies, processes, procedures, standards, guidelines and awareness programs. Our defense-in-depth strategy is composed of the following seven layers:

- A perimeter security layer, which deploys gateway protections where we connect to the external world;
- A network security layer, which houses the cybersecurity protections on our internal network;

- An endpoint security layer, which includes the security tools and technologies deployed on our laptops, workstations and mobile devices;
- An application security layer; which are the controls around our Social Security software applications;
- A data security layer, which are specific protections around our data;
- A prevention layer, which are those processes that allow us to identify gaps in our cybersecurity posture and address them; and
- A monitoring and response layer, which includes the protections in place to identify and respond to an incident.

Federal Cyber Sprint and the Cross-Agency Priority CyberSecurity Goals

I will now discuss the Agency's performance on the Federal Cyber Sprint and the Cross-Agency Priority CyberSecurity goals.

Cyber Sprint of 2015: We continue to build on the work we initiated last July as part of the federal Cyber Sprint. During the Cyber Sprint, agencies focused on multi-factor authentication, privileged users, remediating critical vulnerabilities identified by DHS, and assessing high value information assets. A brief status of our efforts is below.

Multi-Factor Authentication - Personal Identity Verification (PIV) cards
One way to enhance the protection of agency data is to ensure employees utilize their Personal Identity Verification (PIV) card when logging onto agency computer systems. This two-factor authentication method makes it harder for unauthorized individuals to gain access to SSA's network and systems and better protects sensitive agency data. We have issued PIV cards to 100% of the privileged users and 88% of unprivileged users on our network. We have a plan for completing the issuance of the remaining group of users in the State Disability Determination Services (DDSs) by December 2016.

Privileged Account Management
During the Cyber Sprint, we reduced the number of network privileged users in the Agency by 10 percent, and we continue to focus on controlling privileged accounts. Privileged accounts are user accounts with administrative privileges that possess a greater level of access than a regular user account. SSA is deploying new technology, which will allow us to control privileged accounts to a much greater degree, by letting users check out privileges only when needed, instead of having them assigned permanently. This will reduce the risk of these privileged accounts being compromised and used for malicious purposes.

Remediating Critical Vulnerabilities
The Agency was an early adopter of cyberhygiene scanning by the DHS. Weekly and on an ad-hoc basis, as needed, DHS scans SSA-owned IP ranges for vulnerabilities. SSA is one of ten Chief Financial Officer (CFO) Act Agencies that do not have any critical vulnerabilities as identified on DHS' Federal Cyber Exposure Scorecard.

Assessing High Value Assets
We assessed and prioritized the SSA systems and data sources that utilize PII. We conduct regular security assessments of our high value assets including vulnerability and penetration tests. We are currently undergoing our second exercise with DHS to assess the controls around our highest value assets. Such assessments are designed to emulate the attacks of real-world adversaries.

Cross-Agency Priority (CAP) CyberSecurity Goals: SSA meets all nine of the CAP CyberSecurity Goals. These goals focus on the implementation of the continuous monitoring of hardware assets, software assets, configurations and vulnerabilities, the implementation of multi-factor authentication, and malware and anti-phishing defenses.

Cybersecurity Best Practices at SSA

We are often asked to share some of our best cybersecurity practices with other federal agencies. The following section outlines some of those practices.

Incident Response and our Security Operations Center: We have a robust Incident Response Plan that details the roles and responsibilities of Agency personnel involved in a response to a cyber incident or breach. These roles include personnel from all facets of the agency, including our Security Operations Center (SOC). The agency has an internal Security Operation Center (SOC) staffed without interruption that monitors the agency's network environment to identify and detect suspicious activities, react to potential cybersecurity incidents, and ensure uninterrupted service delivery. The SOC leverages many technologies and capabilities to enable fast and accurate threat detection, remediation, and response to security incidents across the enterprise. Best practices in our SOC that we have shared with other federal agencies include:

- A centralized repository and automated workflow for reporting PII loss incidents within the Agency and for reporting all suspicious incidents to US-CERT.
- An automated solution that monitors when any user may be sending PII outside of the Agency in a non-secure manner. The program alerts and notifies management of any user that violates agency policy.
- Dashboards using a data aggregation tool that allow for trending incident data and reporting to agency executives. These metrics and reports improve executive decision-making by highlighting anomalies and providing data visualization.
- A strong working relationship with US-CERT while sharing information on all cyber-related incidents.
- Regular incident response exercises for both internal incidents (discovered by SSA) and external incidents (discovered by a third party). These tabletop exercises simulate the agency's response to an incident. Each scenario identifies roles and responsibilities of specific SSA parties or components for each particular situation and provides a low-stress opportunity to practice incident response.

Enterprise Penetration Testing Program: One of our most effective information security defenses is our Enterprise Penetration Testing program, which we implemented in 2012. It has become a cornerstone of our cybersecurity program to defend against hacks and data breaches. Penetration testing is the method of evaluating the security of a computer system or network by

simulating an attack from malicious outsiders who do not have authorized access to our systems and insiders who have some level of authorized access. The process involves analyzing the system for potential vulnerabilities that result from system misconfigurations and software flaws, both known and unknown. We have a dedicated team of cybersecurity professionals that performs tests in an attempt to "hack ourselves" on a scheduled and on-going basis. The penetration testing process provides the Agency with a third layer of defense beyond our basic cyber hygiene practices of software patching and vulnerability scanning.

This program includes both overt and covert penetration tests, utilizing real-world scenarios. We continually evolve our penetration-testing program as new threats emerge. We track, monitor, and remediate all identified vulnerabilities. Further, we scan all public facing applications for vulnerabilities prior to releasing them to production. We leverage the responses to regularly scheduled exercises and tests to mature the posture and performance of our Security Operations Center.

We also work with outside auditors and provide them access to our systems if requested to perform independent testing. We remediate the vulnerabilities identified by the independent auditor, and we actively detect and remediate additional vulnerabilities both internally and externally. It is important to note that auditors have had no success in breaking into our systems from the outside.

Malware and Anti-Phishing Defenses: The Agency defenses for malware and phishing are a critical component of our cybersecurity program and build on our layers of defense and risk based approaches. We take a holistic approach, incorporating malware and phishing defenses into the various layers of protections at the perimeter, network, end-point, data, prevention, and response layers. We deploy a variety of technologies to detect potentially malicious activity at our gateways to the external world as well as within our internal network. We configure our infrastructure and place controls on user activity to limit the impact of potentially suspicious actions. Some specific best practices are:

- The deployment of multiple technologies to automatically detect and remediate known malicious software at the virtual entry points into our infrastructure.
- The early adoption and continued upgrade of our Trusted Internet Connection and the deployment of the DHS Einstein program to identify malicious traffic targeting SSA and prevent it from harming us.
- The implementation of an enterprise wide social engineering program that tests our employees' ability to recognize suspicious email messages and phone calls. We test all employees once a quarter with phishing exercises to continuously reinforce their skills.

Authentication for *my* Social Security: As the Acting Commissioner mentioned in her testimony, SSA has a robust set of on-line services for citizens to use to conduct Social Security business. We have offered a multi-factor authentication method for citizens to use to access services since fiscal year 2012. This summer, we will make multi-factor authentication mandatory for users. All customers must enter a username, password and a one-time passcode texted to a registered cell phone in order to access their *my* Social Security account. This will ensure that the Agency on-line portal is consistent with the CyberSecurity Act of 2015, the

National CyberSecurity Action Plan, and Executive Order 13681. We are working with NIST and other Federal agencies to identify improvements to the authentication process.

FISMA Compliance and Performance

FISMA mandates that we implement an effective information security program and requires us to regularly assess our major IT systems and report the assessment results in an annual report to OMB and Congress. Our defense-in-depth cybersecurity program ensures that we manage information security risks on a continuous basis, as directed by OMB. In a network of our size and complexity, something can always be better secured. In accordance with FISMA requirements, an independent auditor evaluates our information security program and systems annually. Over the years, these evaluations have found us to be in compliance with the law, but like any audit, have identified areas for improvement.

Our inspector general (IG) contracted with an independent auditor to complete the FY 2015 FISMA audit. The evaluation determined that we established an information security program and practices that were generally consistent with FISMA requirements. However, our overall score was lower than FY 2014. In June 2015, the scoring metrics used by the IG to calculate our FISMA score changed. In total, 21 individual metrics were eliminated—in each of which we had a passing score in FY 2014. This change in scoring methodology contributed to an overall decline in Federal agency scores. With the new methodology, we ranked sixth out of 24 CFO Act agencies with an overall score of 84 points. This year, the methodology will change in another area. FISMA scores will continue to reflect changes to the methodology. Agencies may need time to understand the new methodology and improve effectiveness based on these changes.

The majority of our reduced compliance metrics fell into the area of Risk Management. Throughout the evaluation, we engaged the auditor to explain our approach, provide documentation of our progress, and obtain feedback on their assessment. The auditor noted in FY 2015 that we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources. We also improved our existing controls and implemented new controls and risk management processes in FY 2015. We completed actions on many recommendations from the FY 2014 and FY 2015 FISMA assessments and continue to address open recommendations.

In response to our auditor's findings and recommendations, we expanded our penetration-testing program to include the analysis of external threats in addition to internal threats. We implemented a zero tolerance policy for weak credentials as we further refine our threat and vulnerability management program. We continue to emphasize prioritization and implementation of risk mitigation strategies and plans of action and milestones as we remediate vulnerabilities.

We continue to improve and standardize governance processes for IT applications within the agency. We established improved criteria for assessing the risk and security of applications. These steps help ensure our risk management requirements are effectively and consistently implemented across the organization. This includes our State DDSs, where we are accelerating

the expansion of our suitability clearance process. We also implemented an automated, standardized DDS security plan template that each DDS completed. Given our competing needs and limited resources, we follow best practices and prioritize our actions for improvement to address the most significant risks first.

Conclusion

Again, thank you for the opportunity to testify about these important issues. To summarize our IT security program, I will reiterate that we have a holistic, integrated, defense-in-depth program that ensures we practice good cyber hygiene through constant patching, monitoring, scanning, alerting, and awareness training. While continuing these basic practices, we must constantly add new layers of technology and automation to reduce our reliance on outdated manual processes.

As the threat level evolves and escalates, all organizations must respond with newer and innovative defenses that will improve our ability to respond quickly. Our future cyber program will include the use of more analytics tools to identify threats faster and the use of automation to respond and remediate incidents more quickly.

We have increased the amounts that we expend on cybersecurity programs over the last three fiscal years. However, our resources are constrained, and we need adequate resources and funding to maintain and improve our vitally important cyber defenses and protect the PII of all of our citizens.

Thank you and I am happy to answer any questions.

Chairman CHAFFETZ. Thank you.

Ms. Stone, you are now recognized for 5 minutes.

STATEMENT OF GALE STALLWORTH STONE

Ms. STONE. Good morning, Chairman Chaffetz, Ranking Member Cummings, and members of the committee. Thank you for the invitation to testify today.

The Social Security Administration holds sensitive data for more than 300 million people. It administers programs that result in payments of $2.5 billion per day. It has over 60,000 employees and more than 1,200 field offices across the country. These realities inherently make SSA a tempting target for cyber criminals. Indeed, recent data breaches of government agencies underscore the need for Federal agencies to make every effort to secure and protect sensitive information.

Unauthorized access to or the theft of SSA data could result in harm and distress to hundreds of millions of Americans. While it is a significant challenge to maintain uniform information security controls across an organization as vast as SSA, the agency must continue to make this its top priority.

In our most recent Federal information Security Modernization Act, or FISMA, report, we determined that SSA's programs and policies were generally consistent with FISMA requirements. However, we identified a number of weaknesses that may limit SSA's ability to adequately protect its information systems.

First, there were weaknesses in SSA's network security in that SSA did not always resolve systems vulnerabilities in a timely manner.

Second, inadequate access controls allow programmers to have unmonitored access to various systems functions while other users had in appropriate access to software.

Third, at some non-central office sites weaknesses not only persisted in systems security but in policies and risk management as well.

The risk and severity of these weaknesses met OMB's definition of a significant deficiency in internal controls, a conclusion we have cited in prior SSA FISMA compliance reports. We believe the agency needs to address these weaknesses, as well as strengthen its continuous monitoring program to provide constant cyber protection, prioritize and implement risk mitigation strategies, review and improve account management controls, and enhance IT oversight to ensure consistency across the agency.

It is equally important that SSA authenticates its users of its electronic services. SSA provides many of its customer service functions online through the My Social Security portal, including the ability to change direct deposit information. In recent years, we have received reports of changes to online accounts that beneficiaries did not make or authorize. We've also investigated many cases involving the fraudulent redirection of Social Security benefits to financial accounts controlled by identity thieves. Electronic fraud schemes such as these can affect a significant number of victims and lead to large Social Security losses.

While SSA has taken steps to strengthen controls over the My Social Security portal, given the sensitivity of the information in

these accounts, SSA should implement additional user authentication techniques to further guard against identity and benefit theft.

Finally, SSA must properly manage its IT investments to position itself for success. SSA expects to complete its systems migration to the new data center in August. This modern data center should meet SSA's IT needs for at least 20 years. OIG provided real-time oversight of this project to help ensure that it was completed on schedule.

The disability case processing system, however, has been in development for more than 5 years. Last year, SSA reset the project and it continues to work on a single case processing tool for disability examiners across the country. To date, SSA has spent more than $300 million on DCPS, so going forward, the project requires diligent oversight and continued user involvement.

In conclusion, OIG will continue to monitor these issues closely and work with SSA and the committee to enhance and protect the agency's information systems. Thank you again for the invitation to testify, and I'm happy to answer any questions.

[Prepared statement of Ms. Stone follows:]

Good morning, Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee. Thank you for the invitation to testify today, to discuss the Social Security Administration's (SSA) information security management and information technology investments.

The Office of the Inspector General (OIG) for many years has placed oversight of SSA's information technology infrastructure among its top priorities. During my tenure in the OIG's Office of Audit, I directed and oversaw our financial and information technology audits of SSA's operations, and I have served on the National Institute of Standards and Technology's (NIST) Information Security and Privacy Advisory Board, so I appreciate the opportunity to discuss these critical issues with your Committee.

Protecting Government Information Systems

Government information systems, and the data they hold, are increasingly becoming targets of cyber attacks. Recent data breaches at government agencies have underscored the need for Federal agencies to make every effort to secure and protect sensitive information. In recognition of the rapidly increasing importance of government cybersecurity, Congress passed the *Cybersecurity Act of 2015.*[1]

It should come as no surprise that SSA—like other Federal agencies that collect and store voluminous amounts of personal information—could be a potential target for a cyber attack. The Agency houses sensitive information for nearly every U.S. citizen—living and deceased—including individual medical and financial records. SSA maintains 14 general support systems and 8 major applications to conduct its business, and it has tens of thousands of employees interacting with citizens in more than 1,200 field offices across the country.

While it is undoubtedly a significant and ongoing challenge to maintain uniform information security protocols across an organization as vast and complex as SSA, it is a challenge that must be met and remain a chief concern to Agency leadership and the OIG. Inappropriate and unauthorized access to, or theft of, SSA data could result in severe harm and distress to potentially hundreds of millions of Americans.

Last year, SSA provided about $930 billion in payments to about 67 million Americans; almost all of these transactions are electronic, and SSA encourages its customers to interact with the Agency though online services to apply for benefits, to input and edit direct deposit information, or to request a replacement Social Security card, for example. As it conducts more business online, SSA must ensure that it properly authenticates customers and secures transactions.

The *Federal Information Security Modernization Act of 2014* (FISMA) requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the data and systems that support the agency's operations and assets. The law also requires inspectors general to evaluate its agency's information security programs and practices on an annual basis, to include internal and external penetration testing of agency systems.

My statement will focus on the results of our most recent report on SSA's compliance with FISMA, though we have conducted many other reviews on SSA's information technology infrastructure, such as

[1] The law, among other things, established a voluntary framework for the sharing of cybersecurity threat information between and among the federal government, state governments, and private entities.

authentication and security controls over its electronic services, as well as SSA's major information technology investments, like the National Support Center and the Disability Case Processing System.

SSA's FISMA Compliance

In our most recent report on SSA's compliance with FISMA, we determined that SSA had established an information security program and practices that were generally consistent with FISMA requirements. However, we identified a number of deficiencies that may limit the Agency's ability to protect the confidentiality, integrity, and availability of SSA's information systems and data.[2] The deficiencies identified are consistent with those that we have cited in prior reports on SSA's FISMA compliance.

Before I review the reporting metrics that revealed significant deficiencies in SSA's information security controls, I want to highlight the importance of the Agency's efforts to implement NIST's Information System Continuous Monitoring (ISCM) strategy. Continuous monitoring helps organizations maintain ongoing awareness of information security, vulnerabilities, and threats to support risk-management decisions. ISCM calls for organizations to implement tools and processes that maintain situation awareness of all systems; maintain an understanding of threats and threat activities; assess all security controls; collect and analyze security-related information; and communicate security status across the organization.[3]

We reported that SSA has "defined" its ISCM strategy, but the Agency continues to rely on manual and procedural information-security methods in situations where automation may be more effective. ISCM requires active risk management by organizational officials, and it is most effective when automated, however we recognize that many aspects of the strategy, especially for legacy data systems as entrenched and complex as SSA's, are not easily automated. SSA's commitment to implementing a comprehensive ISCM strategy—to provide ongoing security monitoring and updates—is of critical importance. Considering the current threat of cyber attacks facing government agencies, a thorough continuous-monitoring program is necessary in any information security system.

Of the 10 FISMA reporting metrics, we cited significant deficiencies for SSA in configuration management, identity and access management, risk management, and security training.

Configuration Management

We identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner. I should note that, because disclosing specific details about these weaknesses in a public venue might further compromise controls, we provided those details to SSA management in a limited-distribution letter separate from our report.

Related to this issue, in a separate review of SSA's patch-management process, we found the Agency did not have a comprehensive patch program, thus it did not always address known vulnerabilities timely. Without an effective patch-management process, to include clear policies and procedures and assigned roles and responsibilities, SSA's systems are at risk of unauthorized access.[4]

---

[2] Under a contract the OIG monitored, an independent certified public accounting firm audited SSA's compliance with FISMA for fiscal year 2015. The OIG was responsible for technical and administrative oversight of the contractor's review.

[3] NIST, *Information Security Continuous Monitoring for Federal Systems and Organizations*, September 2011.

[4] SSA OIG, *Effectiveness of the Social Security Administration's Server Patch Management Process*, September 2014.

Identity and Access Management
We identified numerous issues with logical access controls that resulted in inappropriate and/or unauthorized access to information systems; this included programmers with unmonitored access to production and application transactions, as well as other users with inappropriate access to privileged functions and sensitive system software. Additionally, we identified control failures related to removing terminated employees' access to SSA's network and other systems, and the Agency was unable to track the departure dates for contractors and substantiate the removal of their systems access.

Risk Management
Weaknesses for information system controls for various non-central office sites continue to persist from past FISMA reviews because SSA has not designed, planned, or implemented corrective actions to remediate weaknesses and mitigate risks. These weaknesses include inadequate platform security, inadequate policy/procedural guidance, and inadequate development and implementation of a risk management framework.

Contributing factors to these weaknesses include SSA's lack of a comprehensive governance structure and an organization-wide risk management strategy; an inconsistent implementation of SSA's information security program requirements; and a lack of sufficient IT assessments performed by management.

Security Training
While SSA has established a security-training program that is consistent with FISMA requirements, the Agency does not have an authoritative system to identify and track the completion of security awareness training for employees and supervisors, including those with significant information security responsibilities.

Agency Efforts, OIG Recommendations
In our review of SSA's overall information security program and practices, we concluded that the risk and severity of the weaknesses described constituted a significant deficiency in internal controls over FISMA.[5] SSA has continued to pursue a risk-based approach to information security, and as I mentioned, the issues we found were similar to those we cited in prior reports on SSA's FISMA compliance.

These weaknesses continue to exist, we believe, because of one, or a combination, of the following:
- SSA's risk-mitigation strategies and related control enhancements require additional time to implement or become fully effective.
- SSA has focused resources on higher-risk weaknesses, and thus it is unable to take corrective actions on all prior-year deficiencies.
- Newly designed controls did not completely address the risks and recommendations provided in past reports.
- Information technology oversight and governance were not sufficient.

SSA should make all efforts to address the weaknesses identified. We also made several additional recommendations to the Agency, including:

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

- Continue, as part of the threat and vulnerability management process, to prioritize and implement risk mitigation strategies.
- Analyze account-management controls to determine whether the controls mitigate the risk of unauthorized access, and consider automating the account-management process.
- Continue, as part of the Cybersecurity Sprint initiative, to improve controls over privileged accounts.[6]
- Enhance current information technology oversight and guidance to ensure processes are effectively and consistently implemented across the Agency.
- Improve tracking of completion of security awareness training, especially for employees and contractors with significant information security responsibilities.

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

Authenticating Electronic Services Users

It is equally important that SSA ensure that it has controls in place and properly authenticates its electronic services users, as the Agency offers many of its customer service functions online, including benefit payment delivery through direct deposit.

Through SSA's *my* Social Security account, citizens now have the ability to update their personal records and access their benefit payment information with SSA online. SSA introduced the online account in 2012, and today more than 24.6 million people have registered accounts with the Agency.

In 2013, SSA enhanced *my* Social Security, allowing Social Security beneficiaries to change their mailing address or direct deposit bank information online. Around the time of this change, we began receiving reports of changes to beneficiary address and direct deposit information that beneficiaries did not make or had not authorized.

Since then, we have investigated many cases involving the fraudulent redirection of Social Security benefits through *my* Social Security accounts to financial accounts controlled by identity thieves. In one example, as the result of an OIG investigation with IRS Criminal Investigations and the FBI, a Miami man was sentenced in 2014 to 88 months in prison for using victims' personal information to create more than 900 fraudulent *my* Social Security accounts and then redirect about $700,000 in Social Security payments to bank accounts he controlled.

As this example shows, this is a serious issue, because electronic fraud schemes can affect a significant number of unknowing victims and lead to large Social Security fraud losses; additionally, electronic fraud cases are difficult to investigate, because the perpetrators can carry out this theft from computers or other devices anywhere in the world. In a recent report, we estimated that about $20 million in Social Security benefit payments to about 12,000 beneficiaries was redirected between January 2013 and January 2014; of that amount, about $11 million had not been returned to SSA, as of August 2015.[7]

[6] In June 2015, the Federal Chief Information Officer, through the Cybersecurity Sprint initiative, instructed agencies to implement a number of immediate high-priority actions to enhance the cybersecurity of Federal information and assets.

[7] SSA OIG, *Unauthorized Direct Deposit Changes through my Social Security*, September 2015.

SSA has improved its controls over *my* Social Security by strengthening the account registration process, establishing a fraud analysis team to investigate potential theft cases, and providing fraud awareness training to employees; we continue to review how the Agency safeguards *my* Social Security accounts and beneficiary information.

When notified, SSA generally moves quickly to resolve issues related to account and direct deposit information. However, given the sensitivity of the personal and financial information contained in *my* Social Security accounts—and the hardship that identity theft can cause—SSA reports it is planning to implement additional user authentication techniques to further guard against identity and benefit theft. We also continue to work closely with SSA to encourage citizens to protect their personal information, establish their own *my* Social Security account before identity thieves fraudulently do so, and regularly monitor their accounts for any suspicious activity.

SSA's IT Investments

SSA's spending on information technology in FY2016 totals $1.5 billion, according to the Office of Management and Budget's IT Dashboard; about 65 percent of those funds are dedicated to operations and maintenance; 32.5 percent are dedicated to development, modernization and enhancements; and the balance to provisioned services. The Agency is currently managing 14 "major" investments, including the National Support Center (NSC) and the Disability Case Processing System (DCPS). We have monitored both projects closely, as the projects' successful implementation is critical to SSA operations.

National Support Center

SSA is currently migrating systems from the National Computer Center (NCC) in Woodlawn, Maryland to the new NSC in Urbana, Maryland. The systems moving from the NCC to the NSC contain demographic, wage, and benefit information for almost every American, and the data are essential for SSA to provide its services to its customers.

SSA built and partially equipped the NSC to replace the aging NCC with $500 million provided by Congress in FY2009 under the *American Recovery and Reinvestment Act*. The NSC is a modern, efficient data center that is expected to meet the Agency's information technology needs for at least 20 years. SSA also operates the Second Support Center in North Carolina, which provides data computing redundancy.

The Agency is on schedule to complete systems migration to the NSC in August 2016. SSA and the General Services Administration have successfully managed this significant project thus far. To date, we have not identified any significant issues that would delay migration efforts; however, a seamless transition of data management to the NSC is critical to SSA operations. The Agency should continue to monitor the risks associated with data migration efforts until the process is complete; going forward, it should maintain appropriate data security plans, disaster recovery plans, and access management controls.[8]

Disability Case Processing System

State disability determination services (DDS) evaluate disability claims and make disability determinations for SSA; there are 54 DDSs across the country, and they use various customized systems to process disability claims.

[8] SSA OIG, *Progress Report on the Social Security Administration's National Support Center*, August 2015.

SSA envisioned DCPS as a singular tool for case processing for the DDSs, which SSA believed would simplify system support and maintenance, improve the speed and quality of the disability process, and reduce the overall growth rate of infrastructure costs. SSA launched the project in late 2010 and used an iterative approach to implement DCPS, starting at one test site and expanding to other test sites as functionality evolved.

In March 2014, SSA contracted with a consultant to analyze the project; in June 2014, the consultant reported that SSA invested $288 million in DCPS over six years, but the project delivered limited functionality and faced schedule delays amid increasing stakeholder concerns. SSA continued development and considered several options to complete the project, including whether off-the-shelf software or a modernized version of SSA's software could be integrated into DCPS. At the request of Congress, we followed up on the contractor's report and responded to several questions about the project. In November 2014, we issued a report and recommended that SSA suspend DCPS development while it evaluated project alternatives.[9]

SSA disagreed and continued developing DCPS, but due to coding and design issues, DCPS functionality remained incomplete. In May 2015, SSA decided to discontinue development and later "reset" the project and changed its technical approach. Teams made up of SSA staff and vendors began redeveloping the system and are currently working in an "agile" environment, which emphasizes collaboration between developers and business experts to incrementally deliver software. SSA's goal is to deliver the first release of the new DCPS system to some—but not all—DDSs by the end of December 2016. However, this "core" release will require DDSs to run parallel systems until SSA develops additional functionality and designs specific customization for many State agencies. State-specific customization proved to be the most complex task in SSA's previous attempt to design DCPS. Accordingly, we have significant concerns regarding the total cost of implementing this system, which, by the time the first release is made available, will total almost $500 million.

We acknowledge that DCPS still has the potential to provide significant value to SSA, but thus far, the project has proven to be very challenging. We continue to monitor DCPS and we will soon issue reports on development costs incurred and SSA's analysis of alternative solutions. Going forward, DCPS needs diligent oversight from Agency management and requires unified strategic decisions.

Conclusion

It is imperative that SSA continues to make protecting its networks and information a top priority; without updated, continuous security, its systems and the sensitive data they contain are at risk. The Agency should continue to dedicate resources to ensure the appropriate design and operating effectiveness of information security controls and prevent unauthorized access to the sensitive information the American public entrusts to SSA.

SSA must also maintain strong authentication controls to ensure that only SSA customers can access online accounts connected to individual personal information and benefit records. Finally, SSA must ensure it properly manages major information technology projects and delivers projects on budget and on time.

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

Oversight of SSA's systems security is a top priority for the OIG. We will continue to monitor these and related issues closely and will work with SSA and the Committee on Oversight and Government Reform to enhance the Agency's information technology security and capabilities, so it can improve operations and serve its customers effectively. Thank you again for the invitation to testify, and I am happy to answer any questions.

Chairman CHAFFETZ. Thank you. Thank you all. I appreciate your testimony but will now recognize the gentleman from Tennessee, Mr. Duncan, for questioning.

Mr. DUNCAN. Well, thank you, Mr. Chairman, and thank you for calling this important hearing.

I remember just a few years ago in this same committee when we had a hearing on identity theft and how fast that crime was growing and we had a witness from a company that had been on one of the morning programs not long before that that this company had downloaded 250,000 Federal tax returns just to show that it could be done.

And so sometimes I wonder if there is such a thing as cybersecurity. In fact, my staffer has one possible—he always writes out many questions for me, but he has got one here: If the government spent most of its budget on just updating and modernizing IT systems, could we ever guarantee that they would not be vulnerable to hackers and malicious code? And I think the answer to that is no. And it seems to me that all this—I don't know if it is almost a waste to keep trying to arrive with cybersecurity that is impossible to obtain.

I also have gotten the figures. The Social Security Administration has spent approximately $16 billion on technology in the last 10 years, $16 billion, and yet I keep reading these things about how their IT infrastructure is aging, out of date. I mean, it just seems crazy to me because the biggest corporations in this country and wants to do business with all 310 million like Walmart and other giant corporations, they spend a lot, but they don't spend as much as the Federal Government does. We have been spending for the last 10 years Federal Government-wide about $81 billion per year.

And it seems to me that these computer companies were turning the top people at these computer companies into not just multi-, multimillionaires but multi-, multibillionaires, and it seems to me that they are ripping off the American people and the taxpayers in the process.

But I do have a question here for Ms. Stone and Ms. Colvin. Would it be possible or logical to put the Social Security Administration's most sensitive information into an intranet system that would be accessible only to government agencies with proper clearance, intranet instead of internet? Ms. Stone, do you understand that question? Would it be possible to do something like that, or Ms. Colvin?

Ms. STONE. I would defer to the agency on that because I would say that that's the environment that we have now is that it is intranet. But again, I will defer to the agency.

Ms. COLVIN. Sorry. The system that we have now is—you know, is available only to those who are given access to it, which is primarily our employees. We share data with other governmental agencies and some local and State agencies.

I would ask Rob Klopp, who is really our technologist, to talk about other ways ——

Mr. DUNCAN. All right.

Ms. COLVIN.—that this might be done.

Mr. DUNCAN. All right.

Mr. KLOPP. So what we try to do today in order to authenticate people is the same kinds of things that commercial companies do. We will reach out and ask interesting questions that come from your financial background through contracts with folks like Equifax and Experian. So if you try to set up a My SSA account, what we do is ask some question about, you know, when did you start your mortgage on your house at such and such an address, I mean, things that are very difficult for bad actors to get a hold of.

So—and as Marti pointed out, the next level of this authentication is to use two-factor authentication, and we're going to mandate that on My SSA in the middle of this year.

So, you know, I think that we're trying to do—you know, we're bringing on all of the best practices to do the best we can to try to cut down the identity fraud, which is what happens when people can get in. It's not really a cyber thing, but it's definitely something that as CIO that I'm trying ——

Mr. DUNCAN. Well, my time is up, but I just think it is so frustrating to see all of this spending, much more than is being done in the private sector, and yet we are not hearing the same excuses from the private sector. And I know the easiest thing in the world is to spend other people's money and there is just not the same pressures or incentives to hold down spending in the Federal Government as there is in the private sector. But we have got to do better. We can't keep getting with all the spending, these—hearing over and over again that the systems are out of date, aging, and so forth. Anyway, thank you, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the ranking member, Mr. Cummings, for 5 minutes.

Mr. CUMMINGS. Thank you very much.

I want to just follow up on what Mr. Duncan was just talking about. I think he makes a very good point. I mean, when you look at this situation, it seems that we are spending a lot of money. And I believe that the money is probably being spent effectively and efficiently, but I also think that we are—we heard testimony yesterday that it is almost like trying to fix an airplane while you are flying it, you know, create it while you are trying to fly it because you are always trying to keep up with things.

And, you know, listening to Mr. Duncan, it is interesting to note that in the private sector, look at folks like Home Depot and others, I could just name all the private folks who have had their systems hacked very effectively.

So can you answer his question, though? I mean, how do we—is it too big to properly address, this whole issue? In other words, the thing that I think that concerns me is the image will be presented that we are just spending, spending, spending, and then the people on Capitol Hill, that is us, come to that conclusion, and then you end up not getting the money that you need. And then of course we are going to beat up on you when you are not answering the calls, when you are not addressing all the issues that you have to address. So somebody make the best case for me, please.

Ms. COLVIN. I think it's very clear that hackers and bad people are going to constantly try to infiltrate every system, just as you

had the Fosters, and I think that we have to be as determined that they will not, and I think that's the reason for the rigorous testing, why we try to hack ourselves, why we use independent auditors, and why we work very closely with Homeland Security because each time a vulnerability is identified, we address it immediately or as resources permit.

And I think that this is something that we have to constantly do. We're in an evolving environment where technology is certainly continuing to develop. We've had to move away from the paper process so it's not like we have options of not using the technology. So we have to constantly look at best practices, constantly make sure we have the expertise that we need inside the agency. I think SSA is fortunate to have someone who's come from corporate America who has worked with a lot of the technological changes and will help us to move forward.

We know that it's a continuous, ongoing process. We do believe—and I'll let Rob speak to this, but we do believe that because our legacy system is so old, we are at risk and we need to make changes, but we have to make them carefully because we can't run the risk of not being able to get the $930 billion out. And Social Security has never missed a check payment, and we use that old system to do that.

I think also there's been a new way of procuring and developing systems thanks to the work of the Congress and others so that you have more agile development and that you can look at the cybersecurity issues and what you need to do to address those.

Rob, you want to add something to that?

Mr. KLOPP. You know, I think Marti pointed out that, you know, cyber is an ongoing effort. I think that part of the deal is that we probably started off a little bit behind, and we need—and we're catching up, but I'm talking about the Federal Government in general, not about SSA in particular. And I think we are catching up.

One of the side effects of having electronic information is that it—you know, it is vulnerable. So we're working on it. I think we'll continue to work on it. I think that the benefits of technology outweigh these risks by so much that we just have to keep on it and keep being vigilant.

Mr. CUMMINGS. Let me ask you, Ms. Stone, I want to move on to you. I understand that resource constraints have also affected the inspector general's office, including its IT security efforts. Most of the people on this committee, by the way, have a phenomenal amount of respect for IGs. We try to be as supportive of you all as we possibly can be.

Your office first approached creating a Computer and Internet Security Incident Response Team in fiscal year 2015 budget request, but this request has not been funded, is that right? And what role would that—what would have been the role of that team?

Ms. STONE. The vision of that team would be to assist the agency in the event of some type of cybersecurity incident.

Mr. CUMMINGS. And so as a result of not having the resources, what are the consequences?

Ms. STONE. We don't have agents to dedicate to that—to those events.

Mr. CUMMINGS. And was that a top priority of yours?

Ms. STONE. Well, that along with I just—generally building that—an infrastructure around electronic information as a whole where we're using data to identify potential vulnerabilities and working with the agency to, I guess, improve its continuous monitoring program, just providing that constant feedback to them on where they're—we see vulnerabilities.

Mr. CUMMINGS. I am running out of time, but let me ask you this. You made a number of recommendations. Do you see a lot of this being the result of fiscal issues, in other words, not sufficient funds? I mean, I'm just curious ——

Ms. STONE. Well, I ——

Mr. CUMMINGS. See, because that is why we call you up here is that we keep throwing money but that we don't see a lot of progress. And so therefore, again, as I said a little bit earlier, then folks say let's reduce the money. And so I am just—you are the one making the recommendations. Your budget—I know you have been affected based upon what you just said, but what about your recommendations with regard to the agency?

Ms. STONE. Well, what I can say is that we have seen a conscious effort by the agency to address issues like limiting the privilege accounts that have higher access. We've seen them work on continuous monitoring. We've seen them, I guess, implement additional multifactor authentication. So there is a willingness on the agency's part to address these. I can't really speak to their budgetary use, but we have seen the efforts on their part.

Mr. CUMMINGS. Just one last thing, Mr. Chairman.

You know, one of the things that I tell my office is that, you know, a lot of times the public has come to the point to have low expectations of government. They don't expect to get somebody on the phone. They don't expect things to be addressed properly. And then the complaints, Commissioner, as you know, then come to us.

And I think, you know, this whole idea of trying to do all the other things that you have to do, that is address the calls, and I know you get a lot of them, the complaints, the problems, but you have got to have people and you have got to have resources to do that. And so what happens if you don't have the resources, if you don't have the people, the quality of service has to suffer. I don't care—no matter where—I have managed a lot of people in a lot of offices, and it has to suffer.

So, again, my thing is making sure that the resources that we do have are used in a way that is effective and efficient. And again, that is sort of an offense of defense because, again, these folks here, they will cut you—I mean, you won't have a budget. And folks will be saying, you know, again, do more with less. And you all have to constantly, and you know this, make the best case for the funds that you have and the funds that you need.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize myself for 5 minutes.

One of the concerns—I do agree with Mr. Cummings that one of the deep challenges is you are flying an airplane and the capacity of that airplane continues to grow. And one of the big concerns we have is we have to do the inspections, we have to worry about the penetration tests. At the same time, we have got a constant need

in the IT sector to upgrade. So I do understand and respect that, but I do believe also that we, particularly in Congress, rely heavily on the inspector general to be the impartial eyes and ears on the ground.

Ms. Stone, I want to talk about one of the penetration tests at Social Security Administration. This was a test conducted by the Department of Homeland Security. It was done at the request of the agency, and it was done in August 2015. When did your office first learn about this test?

Ms. STONE. We were actually briefed on these tests in September 2015.

Chairman CHAFFETZ. So you were given a verbal briefing in September, roughly a month after the test, correct?

Ms. STONE. Right.

Chairman CHAFFETZ. And when did you first get a copy of the report?

Ms. STONE. Within the last 2 to 3 days.

Chairman CHAFFETZ. From just now, right?

Ms. STONE. Yes.

Chairman CHAFFETZ. And where did you get a copy of that report?

Ms. STONE. I believe my chief of staff requested it from a component within the agency.

Chairman CHAFFETZ. And I believe that—did you even know that there was a report?

Ms. STONE. We did not.

Chairman CHAFFETZ. How did you learn that there was a report?

Ms. STONE. In conversations with members of your staff.

Chairman CHAFFETZ. So now that you have had a chance—it is our staff that lets you know that there is a report. You get a verbal briefing. You don't know that there is an actual report. We let you know that there is a report, and then now that you have gone through that report, do you think that the verbal briefing accurately portrayed the results of that test?

Ms. STONE. Well, at this point I would say we haven't had an opportunity to do a deep dive on the report, which is why we need to look for any inconsistencies. There was some language used in there in the report, as I understand it, that was not consistent with what we received during the verbal briefing, so we wanted to make sure that we have an opportunity to evaluate that report. And because we have our contract auditors doing their annual FISMA review at this time, we will definitely share that information with them.

Chairman CHAFFETZ. Do you think the testers—did you know, for instance, that the testers observed and copied personally identifiable information and were able to exfiltrate that randomly generated return?

Ms. STONE. We did not know that until we had the opportunity to review the report. I believe the earlier briefing suggested that there were no PII.

Chairman CHAFFETZ. That is kind of an important point, do you think?

Ms. STONE. Yes, it is.

Chairman CHAFFETZ. Well, okay. We have got three people from Social Security here. Please explain to us why you didn't let the inspector general know a pretty important part of the test that they were able to exfiltrate data. How can you not share that with her?

Ms. COLVIN. I can't speak to the specific report. Marti—Ms. Eckert will be able to do that. But I do want to emphasize that we invite the auditors and Homeland Security in to test so that we can identify vulnerabilities that we can fix. My understanding is that it's not as if they're penetrating us from outside. We let them in, and then they began to look at how they're going to be able to hack the system and they give us the feedback and then we look at the recommendations of what we need to do.

But relative to your question of why we did not inform the Office of Inspector General, I think Marti probably would be able to talk about what our process is.

Chairman CHAFFETZ. Go ahead.

Ms. ECKERT. Thank you, Chairman. It may be the timing of the briefing that we did as opposed to the actual final written report and why there may have been inconsistencies in what was shared.

Chairman CHAFFETZ. Well, is it not common practice to share those reports with the inspector general?

Ms. ECKERT. We share many work products with the inspector general ——

Chairman CHAFFETZ. I know, but ——

Ms. ECKERT.—even—in ——

Chairman CHAFFETZ. Do you share them or not? You see where it becomes suspicious to us when you have something that is not very flattering, it is embarrassing, I think it is human nature to want to, oh, I hate to share this, but I also do believe that the inspector general is there to help be part of the solution, not part of the problem. And it is suspicious when, you know, you have this report and you don't share it with the inspector general. You went to the lengths to give them a briefing, correct?

Ms. ECKERT. I believe so. I believe that was right at the time that it was occurring, and we were letting them know that that was going on.

Chairman CHAFFETZ. Well, my understanding is that the briefing happened roughly a month after the penetration test started. So here is a copy of the report. "Risk and vulnerability assessment for high-value asset prepared for the Social Security Administration September 28, 2015." Congress shouldn't be the one to tell the inspector general that there is a report. How would they even know to ask for the report?

Ms. ECKERT. So we share over 1,100 different pieces of information from them as part of the financial statement audit. So Ms. Stone referred to the request—that we are doing that again now, and we share everything that is required as part of that audit. We don't necessarily share with them every work product that we produce, and we will know in the future to share those products.

Chairman CHAFFETZ. Well, this was a report produced by Homeland Security?

Ms. ECKERT. Yes.

Chairman CHAFFETZ. It just seems to us—it just comes across as if you are hiding something from the inspector general. The fact

that they were able to, unimpeded, do a penetration test, albeit that you invited them to do it, but that was the finding, is that they were able to exfiltrate personal identifiable information, which means there is a problem and you don't share that with the inspector general. Ms. Stone, is that the way it should work?

Ms. STONE. I would say no. Typically, we have a very good working relationship with the agency, and there is back and forth with sharing information.

I would like to add one point, however, to this is that when we had our contract auditors in performing similar penetration testing, we—those testers also gain access to the point that they could see PII. So the fact that that weakness or vulnerability existed was not news to us, but the fact that there was a report and we had not gotten a copy, that was news to us.

Ms. COLVIN. Mr. Chairman, I will say that, again, we have a very strong relationship with the inspector general as far as being responsive. I always see them as an early alert system. I'm sure that this had to be an oversight because there's no evidence of any history of trying to hide something. It's very possible that the staff was reviewing this so they'd be able to respond prior to sending it to the Office of Inspector General, but we will make certain that that type of breakdown does not occur.

Chairman CHAFFETZ. I appreciate it. We have some more questions about it, but I am well past my time. I will now recognize the gentleman from Pennsylvania, Mr. Cartwright, for 5 minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman. And, Commissioner Colvin, thank you for being here today and for your service.

The President's fiscal year 2017 budget overview states the following—and I want to quote from it because it is concerning—"our current state of service remains fragile as the demands of balancing service and stewardship responsibilities continue to strain our resources." And what does this mean when it says the "state of service remains fragile" at Social Security, if you know?

Ms. COLVIN. Because of budget constraints, we are constantly balancing between our service delivery to the public and our program integrity efforts, which includes cybersecurity. Because of the activity in fraud and the activity in cybersecurity, we've had to continually shift resources to program integrity. For instance, just in 3 years, we've gone from spending $74 million in cybersecurity to $96. That comes away from, of course, our customer service activities, the same thing as we look at developing our systems and other kinds of things.

I had to set up—or didn't have to but I felt it was prudent to set up a centralized fraud unit because fraud was becoming so prevalent in the country and we wanted to be able to get out front and be able to detect it and prevent it, and so we've switched considerable resources there. As a result, we're seeing increased waiting times in our field offices on our 800 number. You will recall that Congress was quite concerned because I had to close a considerable number of offices ——

Mr. CARTWRIGHT. And I wanted to ask you about that because when you say customer service as being basically degraded, that really bothers me. In fact, it says in the Social Security budget overview, "While we have worked diligently to improve national

800-number service, the funding we receive for fiscal year 2016 will increase wait times and busy signals." Commissioner Colvin, that is not acceptable. What is the answer?

Ms. COLVIN. The answer is we need committed, sustained funding. I cannot spend money that I don't have. I cannot incur an antideficiency. We have never made our—for the 3 years we were in a total freeze, and as you well know, it takes 2 years for our workers to even be qualified to do the claims work that we have out there in the field.

When I was here in 1970, we had 70,000 employees. We're down to 62,000 now and at the same time that our workload is continuing to increase. So if we have to pull away from some of the things that we do, it's always the impact on the customer.

Mr. CARTWRIGHT. Well, can you talk about the impact that resource constraints, the type you are talking about, have had on the Social Security 800 number and field offices? For example, how long have wait times been this year?

Ms. COLVIN. I don't know the specific answer to that off the top of my head, but I'd say the average wait is probably 30 minutes. We still have lines in our field offices. We are constantly looking at IT to see how we can take some of the work out of the field offices to be able to address the wait times. For instance, we have 4 million visitors a year to our offices for a replacement Social Security card. We're beginning now to roll out a replacement card online, but we have to do that carefully. We have to make sure it's secure. So we're doing whatever we can to pull out work from the field office to make the wait times less, same thing with the 800 numbers, but it's a resource issue.

Mr. CARTWRIGHT. Well, that is wait times on the phone. Maybe even more important are the people who are waiting for adjudicatory hearings. Can you discuss the impact that the resource constraints have had on wait times for adjudicatory hearings, Commissioner?

Ms. COLVIN. There have been two impacts. One has been our budget and the inability to actually have the number of ALJs we need to have a hearing, as you know, at the hearings require an ALJ. We also in the past years have had difficulty with getting a register of candidates. We're working very closely with OPM, and thanks to Congress, there was a required date for a test, and so that's moving forward.

But at the same time, it's a resource issue. We're now up to 570 days that someone has to wait for a hearing. It's something that greatly concerns me because many of these people die before they get a decision. But again, we try to balance the resources we have.

Mr. CARTWRIGHT. So what happens if Social Security does not receive the funding it has requested? What happens to these wait times?

Ms. COLVIN. They will increase. They will increase. We are very efficient as an agency, and I must stress that. Our overhead is 1.3 percent of all of our outlays. We like to talk about USAA as being one of the best private insurance companies. Their overhead is 8 percent, so I think we do an incredibly good job with the resources we have, and I'm able to tell you how we spend the dollars. But

the bottom line is we do compete with other agencies for the dollars, and we don't have an adequate budget.

Chairman CHAFFETZ. I thank the gentleman.

Mr. CARTWRIGHT. Thank you. I yield back.

Chairman CHAFFETZ. Thank you.

I now recognize the gentleman from Texas, the chairman of the subcommittee on IT, Mr. Hurd of Texas.

Mr. HURD. Ms. Eckert, when was the DHS security review done?

Ms. ECKERT. My recollection is it was done in August. It was last summer.

Mr. HURD. How many critical vulnerabilities were found?

Ms. ECKERT. There were a set of about nine recommendations that they made to us.

Mr. HURD. So you don't know how many critical vulnerabilities were actually found?

Ms. ECKERT. It was a penetration-type test ——

Mr. HURD. Yes.

Ms. ECKERT.—so it wasn't that they were looking for specific ——

Mr. HURD. How long have you been ——

Ms. ECKERT.—software vulnerabilities ——

Mr. HURD. How long have you been the CSIO?

Ms. ECKERT. Three years.

Mr. HURD. Three years? And you have a qualified—and, Ms. Colvin, I want to start with you on a comment. You are right. You all did the right thing by getting a third party to come in and test your systems. That is a good best practice, but you all approached this hearing absolutely wrong. You should have come in here and said, listen, we have X number of critical vulnerabilities from August of 2015 and that these are the steps that we have taken to mitigate all of these actions. And this information was given to the second group of people that came and did another security evaluation.

And you are talking about how you are not properly capitalized, but look, you guys have saved $300 million in IT savings by doing things properly. Good work. But the reality is use the money that you actually have in the right way. You are not giving a team that is coming in here to test your digital infrastructure, and you are not giving them all the information from the previous test.

And not once have you all come in here and said that there are these significant vulnerabilities, critical vulnerabilities that we fix. The DHS team was able to escalate privileges once they were inside their system and take control over your entire system. That is a big deal, all right? And the fact that in none of you all's testimony do you mention this.

And then you have the audacity to say that Social Security meets all of the cross-agency priority cybersecurity goals. Somebody was able to sit on your system and take complete control over it. I wouldn't consider that to be a—I wouldn't pat yourself on the back for being able to perform that. And you are the CSIO and you don't know how many critical vulnerabilities that there were in a report that was done and a test that was done almost a year ago? Please.

Ms. ECKERT. We report our vulnerabilities monthly to the Department of Homeland Security. Every month, the number of ——

Mr. HURD. So what are you doing to fix it?

Ms. ECKERT. We have very many different things that we do. It is a holistic ——

Mr. HURD. You have very many different things?

Ms. ECKERT. It is a holistic, integrated approach. We do patch management, we do intrusion detection, we do ——

Mr. HURD. Okay. Ms. Eckert, you obviously ——

Ms. ECKERT.—continuous monitoring ——

Mr. HURD.—didn't read my background before you came here. I did this for a living, okay, and so saying you have many very different things is not a strategy on how to mitigate critical vulnerabilities.

Ms. Colvin, how many records do you have on the—how many Americans do you have information on?

Ms. COLVIN. We have over 175 million wage earners, and then we have ——

Mr. HURD. How many Social Security numbers are there?

Ms. COLVIN.—about 65 million beneficiaries. We have records on most—on everybody.

Mr. HURD. Pretty much everybody, right?

Ms. COLVIN. Yes. Yes.

Mr. HURD. I think that is a pretty big deal.

Ms. COLVIN. Yes.

Mr. HURD. When you talk about PII, this is the treasure trove a ——

Ms. COLVIN. Yes.

Mr. HURD.—and it should be protected with the best tools. And we should have—I have said this 100 times. This is not an issue of technology. This is an issue of leadership. You have information on every single American in the United States of America, and your CSIO doesn't even know from the last report how many critical vulnerabilities there were. They don't know how many times they were able to escalate privileges. And then the other group that is coming in and you are doing a best practice, you are not sharing that information with the IG? And our subcommittee, our staffers had to inform the IG of this information? This is absolutely ludicrous.

And the reason we have all of you all here is because it stops with you ——

Ms. COLVIN. I understand.

Mr. HURD.—right? This is your responsibility. This is your—you have got to make sure this happens, and if I were you, I hope you have some very uncomfortable conversations with your CIO and your CSIO because this is basic information that they should know. And as a taxpayer, as someone who did this for a living, as someone who was responsible to 700, 800,000 Americans, I am appalled by this. And you know what, if I were the Russians, I were the Chinese, I were other hackers, I would be licking my chops because these people are not prepared to protect this information. This is outrageous.

And, Mr. Chairman, thank you for this. Thank you for the bipartisan nature of this, and I yield back my time.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. HURD. Unbelievable.

Mr. CONNOLLY. Thank you, Mr. Chairman.

I say to the panel some of the frustration you are hearing is not only about Social Security. We have had a series of hearings where we hear the same story, and we are very worried that the Federal Government is so vulnerable.

There is a story on CNN today that the nuclear program of the United States is protected on floppy disks, technology going back to the 1970s, and one asks what could go wrong with that?

So I welcome anyone answering, but following up on my friend from Texas, Mr. Hurd, how worried should we be? I mean, given the fact that you have, as you say, Ms. Colvin, data on every American, to make sure they have the benefits when they qualify that they need and that they are entitled to? But the downside of that is you have got data on every American. And we saw what happened with the OPM breach, which compromised information on people who trusted, you know, their information with a Federal agency for a job application or for Federal service or for a security clearance.

And so help reassure us that we are not facing something similar with Social Security Administration, that Mr. Hurd can be reassured that actually after testing the system whatever the vulnerabilities we discovered we have moved with alacrity to address them in an efficacious way.

Ms. COLVIN. Mr. Cooper, we certainly as an agency are not ——

Mr. CONNOLLY. No, no, I am Mr. Connolly.

Ms. COLVIN. I mean Mr. Connolly.

Mr. CONNOLLY. That is all right.

Ms. COLVIN. I'm sorry, sir.

Mr. CONNOLLY. I am Irish, Virginia, via Boston a ——

Ms. COLVIN. Apologize.

Mr. CONNOLLY.—God only knows what it is. I don't know.

Ms. COLVIN. Let me just assure you that ——

Mr. CONNOLLY. No problem.

Ms. COLVIN.—we are very concerned about cybersecurity in the agency, and we know as an agency—I'm not talking about the rest of the government. As an agency, we are always concerned about this. We know that we're always seeking that continuous improvement. We look at the vulnerabilities to see what the ——

Mr. CONNOLLY. Yes, but, look, I have got a little bit of time. I am seeking reassurance. He raised the question, Mr. Hurd. He was responding, Ms. Eckert, to what he thought he heard from you. I am giving you the opportunity to come back and reassure us you can rest easy because, yes, we discovered vulnerabilities and here is what we did or they have all gone away magically or they are still there and we don't know what to do about them. I mean ——

Ms. COLVIN. Well, I think Ms. Eckert can talk about what we've done, but I just wanted to say that this is an ongoing, continuous challenge ——

Mr. CONNOLLY. Of course.

Ms. COLVIN.—as an agency.

Mr. CONNOLLY. We know that, but ——

Ms. COLVIN. All right. Marti, you want to speak to what we're doing?

Mr. CONNOLLY. Well, what we have done after you got the data you got in terms of the penetration.

Ms. ECKERT. Sir, as I said, we have a holistic and integrated ——

Mr. CONNOLLY. You have got to speak into that microphone, Ms. Eckert, because I can't hear you. I am sorry. Thank you.

Ms. ECKERT. Oh, my apologies.

Mr. CONNOLLY. That is all right.

Ms. ECKERT. We do have an integrated, holistic approach. As far as the specific vulnerabilities, it—identified in the DHS report, they were recommendations that we have taken action on. Specific vulnerabilities that were uncovered have been remediated, but let me reiterate what the commissioner said. We hack ourselves every day, so we look for vulnerabilities continuously with continuous monitoring. We also on top of that then have our own penetration testing program where, daily, we attempt to identify and remediate vulnerabilities that we find over and above our continuous monitoring strategy.

Mr. CONNOLLY. And in the process of doing that, Ms. Eckert, have you identified—you know, we have got some clunky systems that have to be replaced, and here is the program for doing that or here is the need we have identified, and we don't have the resources yet to address that because that is a critical piece, too. We are dealing with legacy systems. We are dealing with non-encrypted systems. I mean, we have got—and, Mr. Klopp, I'm going to get to you on that in terms of implementation of FITARA that tries to address all of that. But, I mean, I hope that is part of what you—it is not a sign of weakness to identify weakness. It is a sign of weakness when you ignore the weakness.

Ms. ECKERT. We do, and we take a risk-based approach to remediating our vulnerabilities and all cyber recommendations that we have, whether they be from DHS, whether they be from the inspector general, whether they are from our own penetration testing program.

Mr. CONNOLLY. Okay. I am now down to 13 seconds.

Mr. Klopp, real quickly, tell us about your FITARA implementation. Your grade improved. We had a hearing on that. And how does that relate to this broader discussion of vulnerability and what we are doing?

Mr. KLOPP. I mean, you know, FITARA is important. I would say we are moving aggressively to fill not just the stuff that is in front of us now and required of us, but we actually think that we are a little bit ahead because we can see the new FITARA stuff that's coming down the pike. You know, again, it's a constant thing.

I guess the last thing I would say is I want—let's be really clear about what we—you know, Marti's pointed out that we invite these folks to come in to test our systems. We take the testing very seriously. And what that means is we want them to find these exposures. We are looking for them to find these exposures.

In both of the cases of the August DHS exercise, as well as our exercise with our other auditors, they were not able to penetrate our system from the outside, and so we let them in. And when we let them in, sometimes they can move around a little bit and they declare the fact that they can move around as a vulnerability but they can't get things out. So we allow them another step and an-

other step and another step because we're looking for these vulnerabilities.

The fact that they found them is because we let them in and we let them in and it turned things off and let them around this because we're looking for these things. We expect to come back to you every time with these auditors finding vulnerabilities because we're—we want them to find them. So we find them, we remediate them.

There's an exercise going on now with Homeland security, and as a result of activities we've taken, we're now more secure than they were—we were the last time in, and they're having a harder time doing some stuff. They've also found some new stuff. And, you know, the next time we come in you can—you talk to us about the new stuff that they've found.

It's—but let me be really clear, and this is—probably the assurances. As far as we know, no one, without help from us, has ever come into the agency, entered and penetrated in or—and exfiltrated data out. No one without help from us or knowledge in advance of the way we have our cybersecurity system set up has been able to do that. So that's the assurances I would give you. They do it when we let them in or we turn off our defenses.

Chairman CHAFFETZ. It scares me to death that you think that. It just really does. It really does scare me because the last time you had that test, they surfed around there for days and they were totally undetected. They were able to exfiltrate data if they wanted to.

I would appreciate it if you would share with our staff in a bipartisan way what you have done to remediate that. We will have to follow up on that.

I will now recognize the gentleman from Georgia, Mr. Hice, for 5 minutes.

Mr. HICE. Thank you, Mr. Chairman.

We all know that Social Security has personal identification information of everyone in America, and I certainly cannot overemphasize the importance of this whole issue to me personally and my constituents, as well as my colleagues here, that the Social Security Administration take cybersecurity seriously and do absolutely everything within your power to mitigate any and all threats that are potential.

And, you know, we are here today because obviously there are some network infrastructure legacy system potential compromising. There are some vulnerabilities is perhaps a better word, and that is why we are here. But any system at the end of the day is only as good as the people who are behind the system and working with it.

Mr. Klopp just referred a moment ago to the August testing and, you know, there are some issues that were found. Okay. We know there are issues. So let me begin, Ms. Colvin, with you. What is the Social Security Administration doing specifically to improve employee training as it relates to the vulnerabilities?

Ms. COLVIN. We have ongoing mandatory cybersecurity training for everyone within the agency. When the—any aberration is detected that has been created by an employee, that is discussed with them, and I think that Marti as our expert can go into more spe-

cific detail, but that is something that we take very, very seriously because we do have offices throughout the country, as well as the local DDS—State DDS's who also have access ——

Mr. HICE. Are you satisfied with the training?

Ms. COLVIN. We are always looking at continuous improvement. When we see something happening that would suggest that employees are not fully in compliance, we do additional trainings. So training is not a one-time thing. It's ongoing.

Mr. HICE. Do you see the FISMA requirements as a floor or a ceiling?

Ms. COLVIN. A floor because I think that we've got to keep up with technology. We've got to always stay in front of the hackers, and that's one of the reasons when Rob talks about wanting to know where our vulnerabilities are, we want to shore those up because we know as soon as we fix those, the hackers are going to probably find something else, and so we went to continuously do that.

Mr. HICE. Okay. So in any given month, how often do you meet with the CIO?

Ms. COLVIN. Oh, I meet with him on a weekly basis many times. I meet with him one-on-one. He's my direct report. He's a member of my senior executive team. We meet on Tuesdays.

Mr. HICE. What about the chief security officer?

Ms. COLVIN. Absolutely.

Mr. HICE. Absolutely what? How often do you mean?

Ms. COLVIN. The—we meet probably several times a week around issues. We—I get a weekly report from Ms. Eckert relative to cybersecurity and what is happening.

Mr. HICE. All right. What about the IG?

Ms. COLVIN. The IG had been invited to attend all of my ——

Mr. HICE. So you feel confident that you are staying in good communication with all these as it relates to the cybersecurity vulnerabilities?

Ms. COLVIN. Absolutely because cybersecurity has to be one of our highest priorities.

Mr. HICE. Yes, it absolutely does.

All right, Ms. Stone, let me go to you. The GAO recently testified to thousands of information security recommendations, and they found that agency had failed to implement those thousands of recommendations even to the extent of 42 percent of the 2,000 recommendations that have been offered. Given your experience in the inspector general's office, what are the problems? What are the challenges? Why are agencies not implementing the recommendations?

Ms. STONE. I can speak from, I guess, experience at Social Security. From time to time you may have a policy or procedure that is managed out of a central office. The ability to replicate that across the country is sometimes challenging. For example, when there have been instances where we've identified a vulnerability in one location, maybe the agency has had an opportunity to come in and remediate it in that location, but because the security posture is not that mature, you may still see that same issue popping up somewhere else. So it really comes down to the maturity of the security posture of the agency in that it's a culture where we are

going to detect it and remediate it as soon as possible and then prevent it from reoccurring elsewhere.

Chairman CHAFFETZ. I thank the gentleman.

We are now going to recognize Ms. Plaskett, the gentlewoman from the Virgin Islands, for 5 minutes.

Ms. PLASKETT. Thank you. Thank you so much. Good morning, everyone.

I thought it was really interesting that your discussion just now, Ms. Stone, about the recommendations and the work that you are going to do and your efforts to replicate these recommendations across the country. But one of the things that I was wondering you had discussed with us today about the critical work that you are performing in the inspector general's office combating waste, fraud, and abuse is the personnel and the amount of individuals that you have. My colleague just stated that systems are only as good as the people that are behind them.

And so I am wondering. I notice that the IG—and I am quoting here in the President's fiscal year 2017 budget—that the OIG employees on duty have dropped from 610 in fiscal year 2006 to 526 in fiscal year 2015. I know that some of that is attrition through retirement potentially and otherwise, but that is a decrease in 84 employees. How has that affected your ability to combat waste, fraud, and abuse at Social Security?

Ms. STONE. Well, first, I will speak to it from an audit perspective. Typically, our auditors are issuing one audit per auditor per year. With the flat-line in our budget and because, I'll say, about 86 percent of our budget is personnel, we've not been able to replace people, so fewer auditors mean fewer audits being conducted. I'd say we've reduced our productivity in that area by about 25 audits.

Ms. PLASKETT. So the funding constraints, they have accounted for some of the flat-lining in productivity or ability to ramp up additional audits, but has it led to any reduction in your staffing as well?

Ms. STONE. Oh, absolutely, especially—I'll speak from an investigative standpoint. Ms. Colvin referred to the Cooperative Disability Investigations unit. We dedicate agents to that project, but we get no additional funding for that. So to the extent that we dedicate another agent to that process, that's fewer agents that can actually respond to a cyber incident or looking at facilitator fraud or things of that nature. So to the extent that our budget remains flat or decreases, that's fewer resources that we have to put on the ground.

Ms. PLASKETT. I have here, and you tell me if this is correct, that the caseload has dropped from 12,000 cases in 2007, and you are saying 8,400 now?

Ms. STONE. Yes, that is correct. Our high was about 12,000 in 2007, and subsequent—and the—I believe the last 3 years we've averaged about 8,400 cases.

Ms. PLASKETT. So I know you know we are all concerned with hacking and infiltration of these systems and our IT systems ramping up, and I know that your office has some integration in that in terms of criminal investigations. Has your office had to re-

duce the number of those investigations due to a reduction in the budget and the flat-lining that you have experienced?

Ms. STONE. Absolutely. Just as you indicated, we've seen that drop from about 12,000 cases to 8,400.

Ms. PLASKETT. And you talked a little earlier when you first started our discussion on Cooperative Disability Investigation program. And my understanding is that that is contract support, correct?

Ms. STONE. Yes. That is a—and the Bipartisan Budget Act actually provided additional funding or language suggesting that there be a CDI unit to cover each State. And when that—those funds come in, it's actually the administrative costs that the agency pays to get those contractors at the State and local law enforcement level. However, for us, none of our personnel or administrative costs are covered for that.

Ms. PLASKETT. And would you say—what would be, you think, a much more thorough—and in your mind the ability to really go after the things that it seems everyone on this panel is concerned about? Would it be through the personnel that are working directly in your office or through this CDI program that they have?

Ms. STONE. Actually, it's a combination thereof because it's a balancing act. Both of those workloads are very important. We've proven that the CDI units are—have a high return on investment, and they're very successful, but by the same token, we still have a responsibility to go after facilitator fraud, and we have to do our normal OIG investigations. So, again, it's a balancing act.

Chairman CHAFFETZ. I thank the gentlewoman.

Ms. PLASKETT. Thank you.

Chairman CHAFFETZ. I now recognize the gentleman from Alabama, Mr. Palmer, for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman.

Deputy Stone, the Social Security Administration reported to staff in a recent briefing that was reported on the Federal IT dashboard—I tell you what, I am going to skip that question. I want to go to acting Commissioner Colvin.

The committee has been corresponding with you about the disability case processing system for years. In a response you sent Representatives Issa, Jordan, and Lankford on July 30, you said, "I have personally and proactively taken to put the DCPS on the right course." Nearly 2 years later, here we are, and so there are a few questions.

And I just want to point out in 2008 started this process of overhauling the DCPS system and spent $288 million and had to scrap it in 2014, basically threw away almost $300 million. I want to know, today, is DCPS currently fully functional serving all of the State DDS's?

Ms. COLVIN. DCPS was started in 2008. As you point out, I assumed leadership role here in 2013 ——

Mr. PALMER. Ma'am ——

Ms. COLVIN.—so it had been in existence ——

Mr. PALMER.—because of ——

Ms. COLVIN.—5 years before I came.

Mr. PALMER. Yes. I did a reset and we are on schedule. We have an aggressive schedule where we expect to be rolling out or having our first product to three DDS's in December 2016.

Mr. PALMER. So the answer is no, it is not fully functional? If you are still waiting ——

Ms. COLVIN. Well ——

Mr. PALMER. Let me ——

Ms. COLVIN. We are doing it in an agile way so products will be delivered on an ongoing basis.

Mr. PALMER. Well, how much have you spent since it has been under your watch since June of 2014?

Ms. COLVIN. That's—I'm sorry, I need to look at that figure. It's about—it's about somewhere between $60 and $70 million on my watch.

Mr. PALMER. Okay. And then you have got another $60 or $70 million yet to spend, is that right?

Ms. COLVIN. Yes, I would say that's accurate.

Mr. PALMER. So do the funding numbers include customizations that Social Security Administration needs to make so that the core DCPS is ready to accommodate the needs of the States?

Ms. COLVIN. We're looking at a core product. There will be some additional costs for customization, but right now, we want to make sure that we have the same product in every State.

Mr. PALMER. But yes or no, does it include the customizations that you need to make?

Ms. COLVIN. I would say yes.

Mr. PALMER. That is interesting. When this is done, how much will Social Security Administration spend on this?

Ms. COLVIN. Are you speaking relative to cost since we reset?

Mr. PALMER. I am talking about total cost, DCPS for the whole ——

Ms. COLVIN. Well, there was $262 million spent by my predecessor, and we're looking at a potential $170 million ——

Mr. PALMER. So we are talking about half-a-billion dollars?

Ms. COLVIN. Not on the reset.

Mr. PALMER. No, I know not on the ——

Ms. COLVIN. Okay.

Mr. PALMER. The total since 2008 we are going to spend about a half-a-billion dollars and we are still not fully functional. So ——

Ms. COLVIN. Well, we started the reset in 2015.

Mr. PALMER. Ms. Stone, what is your view on it?

Ms. STONE. I would say the—my biggest concern at this point is, you know, I don't want to be here answering these same questions 6 months from now. And in the past we've seen some similar situations. I know that they are—that some questions have been raised about whether or not the December time frame is realistic. If we have any delays, that could result in additional cost. We know that this is a complex system. So I'm just as interested and concerned as you all are about the success of this implementation.

Mr. PALMER. Well, there was a McKinsey study of the DCPS that came out in April, April 21, that says that progress had been slower than expected and the current trajectory must be significantly accelerated to meet the timeline for core. Why do you think that is? Why do you think they made that finding?

Ms. COLVIN. Well, I think that clearly it's a complex program. We had had an original management review. We then later had the technical review by McKinsey. They've clearly stated that we're on the correct path.

Mr. PALMER. Let me ask in the few seconds I have left Mr. Klopp to respond to that.

Mr. KLOPP. Sure. So the answer is that we took off on the project starting October 1 of last year. We, for all I think the right reasons, decided to do this in an extremely modern technical environment, which meant that there was a learning curve that we had to take on in order to figure on how to work in the cloud, how to use new programming languages, et cetera, et cetera. And that learning curve slowed velocity in the beginning, as you would expect it to.

What we find right now is that we're passing through that learning curve phase and velocity is picking up, which is why we're so confident that we're going to make the December dates.

Chairman CHAFFETZ. Thank you.

I now recognize the gentlewoman from New Jersey, Mrs. Watson Coleman, for 5 minutes.

Mrs. WATSON COLEMAN. Thank you, Chairman, and thank you to each and every one of you here today.

To you, Commissioner, isn't it true that under the previous Commissioner of Social Security Michael Astrue I believe his name was, the agency made the decision to create a unified IT program system that all DDS entities could use to process claims known as the Disability Case Processing System? Under his tenure, Social Security awarded that primary contract to Lockheed Martin in 2010, is that not true?

Ms. COLVIN. That's correct.

Mrs. WATSON COLEMAN. Rather than have a series of questions, I recognize that we are operating in a very dynamic system, and you have a tremendous responsibility to preserve, protect our information that you have access to and at the same time provide us services. I know in New Jersey we have had problems with the disability office in moving things quickly, but that is what happens.

I also recognize from what I have read that you all have been doing a pretty doggone good job of protecting our information.

Ms. COLVIN. Thank you.

Mrs. WATSON COLEMAN. And there is also a good relationship with the Office of the Inspector General, so you, Commissioner, have taken the opportunity to be a leader and to engage those principles that are very important to the success of your program, as well as the protection of our interests and the delivery of our services.

It changes every day. This system with cyber attacks and things of that nature happens every day. You fix something, people find another way to do it. But yet none of our information has been compromised in the same way some of these large companies, and I need to commend you for that. And I need you to understand that I understand that it is a moving target. And with the right resources, you will keep up with it as much as you absolutely can, but this is not a finite system and this is not a perfect system.

So to each and every one of you, I want to thank you for the dedication and the work you are doing in that space. I yield back.

Ms. COLVIN. Thank you.

Chairman CHAFFETZ. I thank the gentlewoman.

I now recognize the gentleman from Georgia, Mr. Carter.

Mr. CARTER. Mr. Chairman, I want to yield my time to the chair.

Chairman CHAFFETZ. Thank you. I thank the gentleman.

Mr. Klopp, you wanted to provide clarity about penetration and the ability from somebody in the outside to come into the system and exfiltrate information. I want to give you another chance at that. Are you sure that nobody has been able to do that?

Mr. KLOPP. I'm—I will tell you that—Marti and I are passing notes back and forth. We are not aware that they were able to do that in the August penetration—in the August testing that they went on. What I will tell you is that we're undergoing testing today, and I've actually been personally in communication with ——

Chairman CHAFFETZ. Let there be no doubt the two tests of that I am aware that were done at the invitation of the Social Security Administration, they give you credit for the fact that they couldn't penetrate from the outside, but from the inside they certainly could.

Mr. KLOPP. So I believe that when we let them in the inside, they were able to penetrate. They were not able, as far as ——

Chairman CHAFFETZ. So how many people are in the inside? How many users of these accounts do you have?

Mr. KLOPP. Thousands.

Chairman CHAFFETZ. Yes, like tens of thousands, like 96,000 is the actual number. So here is the problem. That is a vulnerability. You had 96,000 people who are already on the inside, and their ability to get in, surf around, and exfiltrate information is undoubtedly happening because the two penetration tests that were tried, that happened.

But I want to talk about from the outside penetration, not the tests, not the people you invited, you are not aware of anybody who has been able to penetrate from the outside uninvited and maybe over what period of time? Any of you?

Mr. KLOPP. I don't think we are—go ahead, Marti.

Ms. ECKERT. So we do not to date have any evidence that someone from the outside has gotten in and exfiltrated out. But anyone in cyber will tell you that there are no absolutes at this point in time.

Chairman CHAFFETZ. Okay. Now, here is the problem I have with that answer, okay, with all due respect. There is a person who is sitting in jail for doing this very thing. There is a person in Miami, right? Oh, now you are shaking your head yes. What happened in that case?

Ms. ECKERT. So that was a case of fraud, correct?

Chairman CHAFFETZ. Yes, it is fraud.

Ms. ECKERT. We're talking about identity theft ——

Chairman CHAFFETZ. Yes.

Ms. ECKERT.—right? And it was identity theft where they acted as someone else ——

Chairman CHAFFETZ. Yes. Oh, yes ——

Ms. ECKERT. Yes ——

Chairman CHAFFETZ.—how creative. I can't believe anybody would do that. What happened? Go ahead. Keep going.

Ms. ECKERT. So there have been—and I think Ms. Stone alluded to ——

Chairman CHAFFETZ. Oh, so there was a penetration from the outside where somebody disguised themselves. In fact, they tapped in and they created 900 fraudulent accounts. How much money did they take out from the government, how much money?

Ms. ECKERT. I don't know the answer to that.

Chairman CHAFFETZ. Yes, it is $20 million. There is $11 million that still hasn't been recovered, and this guy is sitting in jail.

Here is the problem. You are the chief information security officer. The person came in in just the last couple of years and did this. And this is the one that we know about. And you don't recall that off the top of your head?

Ms. ECKERT. So my apologies. I was thinking of cyber incidents and ——

Chairman CHAFFETZ. Why is this not a cyber incident?

Ms. ECKERT. It is ——

Mr. KLOPP. It's not.

Ms. COLVIN. It's not.

Ms. ECKERT. It's fraud.

Mr. KLOPP. It's not.

Ms. ECKERT. It's identity theft ——

Ms. COLVIN. It's fraud.

Ms. ECKERT.—which is fraud.

Chairman CHAFFETZ. Okay. So what is the difference between ——

Ms. ECKERT. And my apologies.

Chairman CHAFFETZ.—fraud and cyber?

Ms. ECKERT. I do understand from your perspective that those things are alike, and my apology for ——

Chairman CHAFFETZ. Well, what is the difference?

Ms. ECKERT. So we have established—we did—we have established an Office of Antifraud Programs, and ——

Mr. KLOPP. So, look, the difference is that cyber is designed to defend us against someone who is coming in trying to hack in through our systems, and that's a completely different ——

Chairman CHAFFETZ. No, it is not.

Mr. KLOPP. No, it is a completely different discipline.

Chairman CHAFFETZ. He came in ——

Mr. KLOPP. It's recognized by the Department of Homeland Security and those folks as a completely different discipline.

Chairman CHAFFETZ. He came into the system ——

Mr. KLOPP. He ——

Chairman CHAFFETZ.—he hacked his way into the system ——

Mr. KLOPP. He didn't hack his way into the system. He did not hack is way into the system.

Ms. COLVIN. No, he didn't.

Mr. KLOPP. What he did was he captured somebody else's identity and came in through the system legitimately as a fraudster. It is not within the—it's not recognized in the information technology world that that is a case of cyber attack. That is not the way the

information technology world would view that. It is fraud. It is identity fraud, and it ——

Chairman CHAFFETZ. He did ——

Mr. KLOPP. He did something that we are diligently fighting against but ——

Chairman CHAFFETZ. He did ——

Mr. KLOPP.—it's not cyber fraud.

Chairman CHAFFETZ. He didn't do this one or two times. He didn't go down the street and grab Betty's telephone number and address and say—he did this by the hundreds of times because he was able to get in there ——

Mr. KLOPP. Because he was able to get 100 identities. Go ahead.

Ms. COLVIN. That was because he was able to get Social Security numbers that he had access to, and that's the big issue of identity theft where you take someone else's identity. But we are now using data analytics to be able to prevent that kind of thing from happening. I've set up a complete center on data analytics where we can look at trends and patterns.

Chairman CHAFFETZ. We will continue to flesh this out with you, but when somebody is able to go in there and change those addresses and do those types of things, I just disagree. I think that is it—that person again, if you are going out and stealing a couple numbers and you are doing that, that is a little different. I would grant you that. But when this person is doing this en masse and changing those addresses—it was the IG that found out about it first.

Ms. COLVIN. It's fraud, though. It's not cybersecurity. We know—I mean, it's a bad issue.

Chairman CHAFFETZ. You've got a lot of ——

Ms. COLVIN. It's one we're working on.

Chairman CHAFFETZ. You've got a lot of explaining to do to us ——

Ms. COLVIN. All right.

Chairman CHAFFETZ.—on how you are differentiating this and who else that should be sitting at this table to protect against that.

Ms. COLVIN. And I would like an opportunity later, maybe not at this hearing, to explain to you what we're doing in those kinds of cases. But we're doing something very differently in dealing with those cases than what we're doing with cybersecurity, and we're working very closely with the Office of Inspector General in those kinds of cases.

Chairman CHAFFETZ. All right. We have a vote on the Floor. I went over my time.

Mr. CUMMINGS. May I have just one ——

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Ms. Stone, with regard to fraud, and perhaps you might answer this, Commissioner Colvin, does finance affect your ability to get to those people who are trying to commit fraud? In other words ——

Ms. COLVIN. Well, it certainly does because when we identify suspicious pattern in a case, we refer that to the Office of Inspector General. And because their resources have been inadequate, they're not able to handle every referral that we make to them. So that definitely would impact their ability to determine what is fraud be-

cause that is their role to determine what is fraud. We simply refer cases that are suspicious or that have a pattern.

Mr. CUMMINGS. Ms. Stone ——

Mr. KLOPP. In fact, it's worth—I'm sorry, it's worth quickly pointing out that when we see fraud, we refer to law enforcement. When we see cybersecurity, cyber breaches, we refer to a completely different branch.

Mr. CUMMINGS. All right. Is that accurate, Ms. Stone?

Ms. STONE. That is correct, sir.

Mr. CUMMINGS. All right. Thank you.

Chairman CHAFFETZ. All right. Two points I want to make and then we will close out here. I was elected in 2008, so that is the benchmark that I take in terms of funding. IT funding for Social Security Administration was about $1.1 billion. It is now roughly $1.5 billion. Everybody wants steady funding. I wish the Congress would move to 2-year funding. I think that would give people more exposure. But that is $400 million more than it was back in 2008.

And so I know there is a lot of discussion about dollars and steadiness and it has been up and down, but it is hundreds of millions of dollars more than it was in 2008. And this penetration test report coming out of Homeland Security, this is—I am going to read this—we have got 11 minutes left on the Floor—on one of the concerns here.

This is from Homeland Security from their report. "Social Security team members were apprehensive about scanning or other rigorous testing of the mainframe due to its fragile operating posture. The DHS team decided to forgo testing of the mainframe in an effort to reduce the operational risk of bringing it down. It should be noted that the fragile state of the mainframe is a major vulnerability on its own and should be addressed as soon as possible."

I think we share a mutual concern of making sure—if they couldn't even get into do a test, how fragile is it? It is an ongoing question, and if you could help answer that question for us.

We appreciate all you do and your cooperation in working with us. We would appreciate it ongoing. We thank you for your participation—Yes. Go ahead.

Mr. CUMMINGS. Just one real quick thing. I have a list of questions, Commissioner Colvin, with regard to EEOC and, you know, I understand that there has been an update on the issue. Can you tell us where we are on that?

Ms. COLVIN. Well, there were two recommendations that we had. One you are interested in what we were doing about the recommendation of EEOC, to have that operation report directly to me. I made that decision, and that will happen effective June 1.

Mr. CUMMINGS. Okay.

Ms. COLVIN. I think the second you have questions about the various EEO class-action cases.

Mr. CUMMINGS. Yes, that is right. The Jensen settlement, which was the disabled employees, has been settled. It is being implemented. The Taylor decision has been appealed on both sides, so we're waiting for a decision to that appeal.

Mr. CUMMINGS. I will have some additional questions which I will submit to you in writing.

Ms. COLVIN. I will be happy to answer those.

Mr. CUMMINGS. All right. Thank you.

Ms. COLVIN. Thank you.

Chairman CHAFFETZ. Thank you. We have some additional questions as well, but we have a vote on the Floor, so the committee stands adjourned. Thank you.

Ms. COLVIN. Thank you so much.

Ms. STONE. Thank you.

[Whereupon, at 10:50 a.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

SOCIAL SECURITY
Office of the Commissioner

September 7, 2016

The Honorable Jason Chaffetz
Chairman, Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your July 18, 2016 letter requesting information to complete the record for the May 26, 2016 hearing titled "Social Security Administration: Information Security Review." Enclosed you will find the answers to your questions.

I hope this information is helpful. If I may be of further assistance, please feel free to contact me. Your staff may contact Ms. Judy Chesser, our Deputy Commissioner for Legislation and Congressional Affairs, at (202)358-6030. I am sending a similar copy to Representative Cummings.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure

Enclosure – P.1 – The Honorable Jason Chaffetz

House Committee of Oversight and Government Reform

Social Security Administration: Information Security Review

May 26, 2016

Questions for the Record for Acting Commissioner Carolyn W. Colvin from Representative Tim Walberg

1. How did the SSA arrive at its cost analysis for ongoing DCPS development?

We used an analogy cost estimating technique to determine the cost of the Disability Case Processing System (DCPS) based on historical data. We used existing costs for Contractor Support Services and extrapolated those costs to fulfill the anticipated need.

a. What are the DCPS's costs to date?

We see DCPS costs in three distinct phases.

The first phase runs from inception of the development of the DCPS project in 2008 to June of 2014. Before becoming Acting Commissioner in 2013, I had no decision-making authority for DCPS. Between 2008 and 2014, a total of $291 million was spent on the project. Upon becoming the Acting Commissioner, I began to learn of the problems with the DCPS project and requested an independent review, which was performed by McKinsey & Company.

The second phase began in June of 2014 after receiving the recommendations from McKinsey & Company at which time I established a separate DCPS Program Office to address the deficiencies outlined in the report. Between June of 2014 to May of 2015, the agency spent $63 million. Work during this phase included introducing a new management scheme, basic Agile Software Development methods, conducting alternative analyses, and engaging the United States Digital Services (USDS) to perform a technical evaluation of the DCPS intellectual property that had been developed. During this phase, we implemented the majority of the McKinsey and Company recommendations.

The current phase began in June of 2015 and is scheduled to run through June of 2019. During FY 16, we project to spend $31million. Working closely with the USDS and the Disability Determination Services (DDSs), we completed agreed upon key major milestones, including defining agreed upon core requirements, and developing the "through line" (the backbone of DCPS). Cumulatively, we will have expended $386 million by September 2016 on DCPS.

b. What are the projected costs for DCPS going forward?

The projected annual development costs for DCPS2 are outlined below.

FY17	FY18	FY19*
$ 34,993,083	$ 39,999,833	$ 16,666,220

**Estimates for FY 2019 are not yet complete and will be updated as additional information becomes available.*

c. What portion of these costs account for the customizations required to meet the state-specific needs beyond the release of DCPS Core?

We are building DCPS in a manner that focuses on the common aspects of states rather than focusing on the differences; this allows us to maintain a common set of capabilities across the DDS community.

Some differences will remain. For these, we will develop customized functionality as we deploy the product to each site – we refer to these customizations as "off/on ramps" because they are not part of the common product.

At this time, our estimated cost for development of "off/on ramps" includes: $5 million in FY 2017; $5 million in FY 2018; and $3 million in FY 2019. The total projected costs for "off/on ramps" is $13 million. These costs are included in the projections listed in 1b above.

d. What are the life-cycle costs of the DCPS included in this projection?

We assume that by this you mean the ongoing cost of running DCPS after deployment. We have budgeted $1.7 million per year for cloud infrastructure, software licenses, help desk support, and other miscellaneous costs. In addition, we have budgeted $5 million per year for two development teams to continuously develop features in support of new requirements driven by the DDSs, such as, evolving technologies, or future legislative and regulatory requirements. Reflected below are our projected annual costs (taking into consideration the time value of money):

FY17	FY18	FY19
$ 6,735,019	$ 6,851,709	$ 6,875,421

2. **The consultant SSA hired to evaluate the DCPS project expressed concern that SSA would likely be unable meet its goal of delivering the first release of DCPS 2 (referred to as "Core") by December 2016; however, at the hearing, CIO Klopp stated he remains confident that SSA is on-target. What steps is SSA taking to address the consultant's concern's/speed up development?**

   As Mr. Klopp stated, we are confident that velocity will continue to improve to allow us to deliver a first release in December of 2016. In fact, velocity has continued to improve. We are working to extend these improvements by adding new experienced contractors and by organizing the work more effectively. Please note that the consultant's concerns imagined no improvement in velocity. However, we have seen increased improvement since the consultant's visit. Working closely with our three early adopter sites, we remain confident that we will deliver our agreed upon product in December 2016.

3. **When does SSA expect to be able to release a version of DCPS that will fully meet the needs of all DDSs, thereby allowing the Agency to retire the legacy systems?**

   The minimum product that will allow a DDS to retire its legacy system will include support for all three case types: initials, reconsiderations, and continuing disability reviews (CDRs). These capabilities will be included in the second release with availability targeted in mid-2017.

   As we work with early adopter states on a rolling basis, we expect DDSs to begin retiring their legacy systems as they complete training and other rollout activities. We anticipate once a DDS deploys DCPS they will retire their legacy system within one year. We anticipate initial early adopter states to be able to retire their legacy systems beginning in late 2017. We anticipate all DDSs will retire their legacy systems by FY2020.

Enclosure – P.4 – The Honorable Jason Chaffetz

4. How much do you estimate DCPS2 will cost, in total? Please include:

(1) costs to develop the eventual version of the application that will permit SSA to retire the legacy systems;

The projected total costs for DCPS2 that will allow DDSs to retire their legacy systems are outlined in the table below.

FY15 (3 Months)	FY16	FY17	FY18	FY19	TOTAL
$ 12,087,901	* $ 30,973,431	* $ 34,993,083	$ 39,999,833	** $ 16,666,220	$ 134,720,467

**Estimates for FY16 and FY17 have been updated based on actual expenditures.*
***Estimates for FY19 are not yet complete and will be updated as additional information becomes available.*

(2) costs to continue maintaining the legacy systems until they are fully retired;

FY15	FY16	FY17	FY18	FY19	TOTAL
$ 31,632,370	$ 33,123,989	$ 34,874,688	$ 36,618,423	$ 38,449,344	$ 174,698,814

The costs detailed above represent the agency forecast for legacy costs each fiscal year. The deployment of DCPS will have a significant effect on these legacy costs. As we begin to deploy DCPS to the DDSs, SSA will realize a reduction of these legacy expenses. It is important to recognize that this is SSA's estimate of the impact to legacy costs in a general sense. We will be able to provide more detailed definition of savings when we begin retiring the legacy systems in the DDSs.

(3) costs to operate and maintain the new DCPS once it has been fully implemented.

We assume that by this you mean the ongoing cost of running DCPS after deployment. We have budgeted $1.7 million per year for cloud infrastructure, software licenses, help desk support, and other miscellaneous costs. In addition, we have budgeted $5 million per year for two development teams to continuously develop features in support of new requirements driven by the DDSs, such as, evolving technologies, or future legislative and regulatory requirements. Reflected below are our projected annual costs (taking into consideration the time value of money):

Enclosure – P.5 – The Honorable Jason Chaffetz

FY17	FY18	FY19
$ 6,735,019	$ 6,851,709	$ 6,875,421

SOCIAL SECURITY

September 7, 2016

The Honorable Jason Chaffetz
Chairman, Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Thank you for your July 18, 2016 letter requesting information to complete the record for the May 26, 2016 hearing titled "Social Security Administration: Information Security Review." Enclosed you will find the answers to your questions.

Due to the sensitivity of the information within one of our responses, we are providing supplemental information in a separate document. We ask the Committee to exclude this supplemental information from the public record as it could potentially be used to compromise our agency security practices.

I hope this information is helpful. If I may be of further assistance, please feel free to contact me. Your staff may contact Ms. Judy Chesser, our Deputy Commissioner for Legislation and Congressional Affairs, at (202)358-6030. I am sending a similar copy to Representative Cummings.

Sincerely,

Marti A. Eckert

Marti A. Eckert
Associate Commissioner, Information Security
Chief Information Security Officer

Enclosure

House Committee on Oversight and Government Reform

Social Security Administration: Information Security Review

May 26, 2016

Questions for the Record for Chief Information Security Officer, Marti Eckert, from Chairman Chaffetz

1. **Since the 2013 incident involving unauthorized individuals accessing others' data on SSA's *my* Social Security application, what has SSA done to improve security of the application?**

   SSA is committed to preventing unauthorized access to its online services and ensuring we safeguard sensitive information. Due to the sensitivity of the information, we are providing you responses under separate cover. A disclosure of our security mechanisms would increase the ability of bad actors to compromise our secure online services.

2. **Have any improvements been made to authentication of new and existing users?**

   Please refer to the information we are providing under separate cover.

3. **Please provide a breakdown of any obligations SSA has incurred to improve authentication and identification of users with *my* Social Security.**

   SSA has an ongoing obligation with our external data source provider, Equifax. This contract supplements our identity proofing and authentication process. In addition, we are using a new service, Device ID, which detects known fraudulent devices.

4. **How do recently completed, on-going, and planned improvements to user authentication on *my* Social Security avoid duplicating existing capabilities provided by the General Services Administration's Connect.gov service, which implements part of the Administration's National Strategy for Trusted Identities in Cyberspace (NSTIC)?**

   We understand that GSA's Connect.gov pilot is not moving forward and that GSA has tasked its 18F digital services team with creating a new federated identity system. As 18F works to create this federated model, we are working in tandem to monitor new Federal guidelines and comply with accepted government standards. We stay in direct contact with 18F staff discussing their plans for a federated model.

   We introduced *my* Social Security in May 2012 before the White House developed the National Strategy for Trusted Identities in Cyberspace. We are not currently working on

any duplicative capabilities similar to Connect.gov or a federated model. We have already put a process in place, but we make enhancements as warranted due to emerging threats. To date, we have over 25 million registered accounts. In an effort to provide service to our customers and to decrease traffic in field offices facing backlogs of work, we continue to allow our customers to create accounts. Once the federated model is a viable solution, we will integrate it into our secure online services platform.

5. **In December of 2015, Congress passed the *Federal Cybersecurity Enhancement Act of 2015* that, among other things, requires Federal Agencies to implement Connect.gov for logons to agency websites by December 18, 2016. What is SSA's progress towards making that deadline with *my* Social Security?**

   We have the infrastructure in place to leverage a federated identity system, once it becomes available. In the meantime, we have developed, and continue to enhance, our identity proofing and authentication system using the most up-to-date Federal guidelines.

Supplemental Information

1. **Since the 2013 incident involving unauthorized individuals accessing others' data on SSA's *my* Social Security application, what has SSA done to improve security of the application?**

   Since 2013, we have taken several actions to improve the security of *my* Social Security. We also have taken agency anti-fraud actions that improve the security of my Social Security. We:

   - Revised the scoring metrics for our external data source provider's (Equifax) Out of Wallet quiz;
   - Created an entire fraud component to detect, deter, and mitigate fraud of Social Security programs along with the policies to support it;
   - Developed a sophisticated fraud detection and prevention process;
   - Added a new suspension policy when fraud is discovered or suspected;
   - Implemented Device ID, which detects known fraudulent devices;
   - Tightened the tolerances in our identity proofing requirements;
   - Implemented an agency-wide block on known fraudulent IP addresses;
   - Enhanced our account block and unblock policies for electronic access; and
   - Added language to strengthen our *my* Social Security Terms of Service.

2. **Have any improvements been made to authentication of new and existing users?**

   See response above.

○