FEDERAL CYBERSECURITY AFTER THE OPM DATA BREACH: HAVE AGENCIES LEARNED THEIR LESSON?

HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

NOVEMBER 16, 2016

Serial No. 114–125

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

24–915 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
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*
MIKE FLYNN, *Counsel*
WILLIE MARX, *Clerk*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

FEDERAL CYBERSECURITY AFTER THE OPM DATA BREACH: HAVE AGENCIES LEARNED THEIR LESSON?

Wednesday, November 16, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:19 a.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the subcommittee] presiding.

Present: Representatives Hurd, Blum, Chaffetz, Kelly, Connolly, and Lieu.

Mr. HURD. The Subcommittee on Information Technology will come to order.

And, without objection, the chair is authorized to declare a recess at any time.

Good morning, everyone. In September, the chairman announced the release of a majority staff report on the data breaches at the Office of Personnel Management. This committee spent a year digging into what went wrong at OPM. We looked at everything from how the hackers got in to what technologies OPM was buying while responding to the incident. And while we learned a great deal, there was an unfortunate conclusion that the damage of this data breach could have been mitigated.

It's impossible to prevent all data breaches, especially when we are talking about a determined and sophisticated adversary. But we can deter and mitigate the effects of these breaches. Some of that, like investigation, attribution, and prosecution, is outside the agency's control. But other aspects, like improving cybersecurity protections and continuous monitoring, are squarely within agencies' CIOs' control. That is why we need to get into the weeds on everything from access controls to vulnerability management to make sure we aren't making it easy for hackers to get access to our sensitive data.

And this is a conversation that starts with the agency's CIO. CIOs are the focal point for all things information technology at every Federal agency, department, office, and bureau. That is why this subcommittee has worked together to ensure the continued implementation of FITARA and, more broadly, making sure that CIOs have the necessary authorities to finally bring Federal systems into the 21st century.

The House recently passed my bill, the MGT Act, cosponsored by Mr. Connolly, Chairman Chaffetz, Ranking Member Cummings, ranking member and my friend Ms. Kelly, the majority leader, the minority whip, and Mr. Lieu from California, which incentivizes agency CIOs to modernize their agencies' outdated legacy IT to fiscal responsibility. I urge the Senate to pass the MGT Act this Congress so that the incoming administration has the necessary tools to modernize our outdated and insecure Federal IT. This is a shared responsibility. Congress can't hold agency CIOs accountable for what's going on in IT if those CIOs don't have the necessary authority to get the job done. We need CIOs staying at their posts for longer than the current 2-year average. If we're going to move the ball forward, we need Federal CIOs not only with the necessary authorities to make their vision a reality but who are sticking around long enough to see it happen. This is why the OPM CIO was such a focus of the OPM data breach report and its recommendations. We need empowered, accountable, and competent CIOs, which brings us to our panel here today.

We need a serious conversation about the role of the Federal CIOs and information security. The President recently announced the creation of a Federal CISO, the Chief Information Security Officer, that will report to the Federal CIO. Should that be a model for Federal agencies, the CISO reporting to a CIO, or should the CISO report directly to the head of the agency? Does the head of an agency need to hear two voices on questions of IT procurement, computer systems, data storage, and balancing the needs of the production environment with those of cybersecurity? This is an open question that this subcommittee has not yet explored. But I think it is an important question moving forward as we continue to conduct oversight of Federal information security policies and practices.

And, finally, we need to address how these agencies transition their information technology over to the new administration. Each agency will have unique challenges. And I would like to hear from our witnesses how they are going to facilitate this transition. We are making progress in information technology and cybersecurity, and I'm committed to ensuring that we don't backslide on this profound national security challenge.

Ultimately, cybersecurity is a collaborative effort that is going to require continuous attention and effort from all parties to make sure our data is safe.

And I'm glad my partner in crime in this endeavor is the gentlelady from Illinois, Ms. Kelly, the ranking member of the Subcommittee on Information Technology and my friend, and I'd now like to recognize her for her opening statement.

Ms. KELLY. Good morning. And thank you, Chairman Hurd, and welcome back. Thank you for holding this important hearing on the state of Federal cybersecurity in the wake of the OPM data breach. And I thank the witnesses for joining us today to testify. Cybersecurity is a critical concern for both the public and private sectors, as the recent breaches affecting millions of people at the Office of Personnel Management and Yahoo illustrate.

In our investigation of the OPM data breach, we discovered that a sophisticated nation-state adversary targeted both OPM and pri-

vate sector companies performing services for the government in order to steal sensitive information about Federal employees. In fact, the OPM breach was achieved using credentials taken from one of our OPM's contractors. The minority staff memorandum concluded that Federal cybersecurity is intertwined with government contractors and that cyber requirements for government contractors are inadequate. In the past 2 years, Congress passed and President Obama signed into law the Federal Information Security Modernization Act of 2014, known as FISMA, and the Federal Cybersecurity Enhancement Act of 2015 known as the FCEA. These laws create stringent standards for agency information security programs and will implement innovative technology, such as the EINSTEIN Federal detection and intrusion prevention system, as well as multifactor authentication—losing my words. Congress has a responsibility to ensure that agencies are complying with these enacted pieces of legislation.

This past July, the committee sent bipartisan letters to the 24 CFO Act agencies requesting information on FISMA and FISMA compliance and FCEA implementation progress. We are here today to discuss agency compliance with FISMA and agency progress on the upcoming December 2016 deadline for FCEA implementation.

I understand that the Office of Management and Budget recently issued a report on FISMA-required independent evaluations of agency information security systems for fiscal year 2015. This report shows a decline in agency FISMA scores over the past year for our three witnesses' agencies here today. Each agency's independent evaluation of their information security programs highlights the strength of their individual programs and areas that can use improvement. One of the key aspects of FISMA is moving from a check-the-box mentality of cybersecurity to an approach of continuous monitoring and reporting. I would like to hear from our witnesses as to how Congress can help them achieve that goal. I would like to hear if any challenges are being encountered in the implementation of FCEA-required programs and practices.

I want to again thank our witnesses for their testimony today. Effective Federal cybersecurity is possible through cooperation between agencies and Congress. I look forward to having a discussion on how we can better work together to develop policies that will secure not only agency systems but private sector systems as well.

Again, thank you, Mr. Chairman. I've long said that Federal Government needs to lead by example when it comes to improving our national cybersecurity. And I'm proud of this step we've taken in this subcommittee toward this goal. But it's clear that we have much more work ahead. And I look forward to continuing our work together in Congress.

Mr. HURD. I do too. I'd like to thank the ranking member.

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

I'd now like to recognize our panel of witnesses. I'm pleased to welcome Ms. Renee Wynn, chief information officer at NASA; Mr. Jonathan Alboum, chief information officer at the U.S. Department of Agriculture—thank you for being here, sir—and Mr. Robert Klopp, deputy commissioner and chief information officer at the Social Security Administration. Welcome to you all.

And pursuant to committee rules, all witnesses will be sworn in before they testify. So please rise and raise your right hands. Raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Thank you. Please be seated.

Let the record reflect that the witnesses answered in the affirmative.

In order to allow ample time for discussion, please limit your testimony to 5 minutes. Your entire written record will be made part of our record.

And now I'd like to recognize Ms. Wynn for 5 minutes for your opening statement.

WITNESS STATEMENTS

STATEMENT OF RENEE P. WYNN

Ms. WYNN. Good morning. Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, thank you for allowing me today to appear before you to address NASA's efforts to effectively manage and protect our information technology resources. Like other Federal agencies, malicious threats to NASA's networks are constantly evolving, which means our work is never done. Thus, I want to reassure you today that IT is a top priority at NASA. As NASA's chief information officer, my office works to ensure that NASA's IT systems are safeguarded from attack, assessed against stringent Federal and agency security requirements, and appropriately monitored for compromise. Each day, thousands of NASA personnel, contractors, academics, and members of the public access part of NASA's IT infrastructure, a complex array of information systems geographically dispersed. This infrastructure plays a critical role in every aspect of NASA's mission, from transforming the way we fly, to controlling spacecraft, to processing scientific data.

Unfortunately, there is no single approach or tool that can predict, counter, and mitigate the wide range of attacks that threaten networks. NASA works constantly to identify and counter attacks by implementing proactive and adaptable security measures. We also work closely with the Department of Homeland Security and other Federal agencies to implement new technologies and share best security practices, partnerships which have improved NASA's security posture. For example, under FISMA metrics, NASA has made improvements in our anti-phishing, malware, and network defense. We have significantly reduced our cybersecurity risk as measured by the Department of Homeland Security's cyber hygiene report. NASA now has a permanent chief information security officer, or CISO, who works on operational IT security and compliance matters with all of NASA Center CISOs, as well as the Federal chief information security officers.

Like all agencies, NASA is adjusting to new laws and directives designed to improve the entire Federal Government's IT security posture. While NASA is making progress in some security metrics, much work remains. As we move forward and find new ways to

work across NASA, our metrics may unfortunately dip as we uncover and we work to resolve new issues. However, as new technologies come online and culture issues are resolved, we expect to see improved metrics in 2017.

Through the implementation of our business services assessment, or BSA, we took a hard look at how we manage IT. This BSA outlined a series of steps the agency should take and is taking to optimize and protect our IT assets. The BSA results will ensure that IT is seen as a strategic agency resource establishing clear direction for NASA's CIO to approve the agency's IT spend plan for non-highly specialized and highly specialized IT. In my personal opinion, this BSA is a gift which says NASA supports you as the CIO, and we do want you to transform the way NASA manages IT.

These are big steps forward for NASA, and NASA should be commended for taking the necessary steps to improve. We know there still is a lot of work to do. Thus, I want to end my remarks by assuring you that protecting and evolving NASA's IT infrastructure is and will remain an agency priority. We look forward to working with Congress, the Government Accountability Office, the NASA inspector general, and other Federal stakeholders to effectively implement a restructured and strengthened IT security program at NASA.

I would be happy to answer any questions you may have.

[Prepared statement of Ms. Wynn follows:]

HOLD FOR RELEASE
UNTIL PRESENTED
BY WITNESS
Nov. 16, 2016

Statement of
Reneé Wynn
Chief Information Officer
National Aeronautics and Space Administration

before the

Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives

Chairman Hurd, Ranking Member Kelly, and members of the Subcommittee, thank you for the opportunity to testify before you today about NASA's efforts to manage our information technology (IT) resources and protect national assets in an ever-changing threat landscape. The NASA Administrator and all of NASA's leadership considers this to be a very high priority.

As NASA's Chief Information Officer (CIO), my office provides IT products and services including policy and procedure for all of NASA. Currently about 17,100 civil servants and 40,000 contractors work at nine NASA Centers and one Federally Funded Research and Development Center, as well as several smaller satellite facilities. We also collaborate with space agencies around the world and have deep partnerships with researchers, engineers and scientists all over the world. Each day, hundreds of thousands of NASA personnel, contractors, academics and members of the public access some part of NASA's IT infrastructure – a complex array of 418 information systems with over 140,000 components geographically dispersed around the globe. This infrastructure plays a critical role in every aspect of NASA's mission, from controlling spacecraft to processing scientific data.

Last year, for example, the entire world watched as New Horizons sent back the first close-up images of Pluto, and we continued to make new discoveries about Mars that will help inform human missions there. This year, the world watched as American Astronaut Scott Kelly returned home from the International Space Station after 12 months of working off the Earth for the Earth. Recently, our Deep Space Network, which relies on NASA's IT infrastructure, was able to get in contact with STEREO-B which had been out of communication with us for over two years. Additionally, this year in space will pay scientific and medical dividends for years to come, helping pave the way for future astronauts to travel to Mars and beyond. The Orion spacecraft and the Space Launch System rocket that will carry us again to deep space continued to reach new milestones. In cooperation with our industry partners Boeing and SpaceX, we moved closer to commercial launches of astronauts from American soil. We are formulating missions to study dark energy, perform galactic and extragalactic surveys and to explore exoplanets. We learned more about our home planet and our challenging climate as newer Earth science missions began to return their data. Technology continues to drive exploration in space and in aeronautics where we have made advances toward a future in which we make air travel safer, cleaner and more efficient.

In support of NASA's many missions, the Office of the Chief Information Officer (OCIO) works to safeguard NASA's IT systems and their associated components from attack, assess them against Federal and Agency security requirements, and continuously monitor them for compromise and for the effectiveness of currently implemented security measures. Given the evolving threat of attacks, our work

is never done. Internal governance and infrastructure changes at NASA have already improved the Agency's security posture, but admittedly, more work remains, especially as the Agency evolves from a highly decentralized IT environment controlled by the Centers and Agency programs and projects to an enterprise IT environment that is more centrally managed and overseen by the Agency CIO.

Therefore, the remainder of my testimony today will summarize key achievements to date, as well as work that is underway to comply with new laws and Administrative directives to all Federal agencies. But before I address those topics, I believe it is important to look at some of the recent governance changes that NASA has made to further empower the CIO to effectively manage its IT network and thus reduce risk of unauthorized access to NASA's assets and data.

NASA IT Governance Changes

NASA is fully committed to meeting the requirements of Federal laws such as the Federal Information Security Management Act (FISMA) of 2002, the Federal Information Security Modernization Act (also known as FISMA) of 2014, the Federal Information Technology Acquisition and Reform Act (FITARA) of 2014, and the Federal Cybersecurity Enhancement Act (FCEA) of 2015, along with additional security directives issued by the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS).

Over the last several years, NASA has made significant progress in updating IT security policies, processes, and procedures to support the ongoing enhancement and automation of information system monitoring and reporting. As a result, Agency IT security staff have obtained more in-depth visibility into NASA systems, enabling improved responsiveness, and further supporting a risk-based security paradigm. Some of the more recent changes include:

- Initiating a Business Services Assessment (BSA) review of how IT is delivered at the Agency (see enclosure);
- Increasing the responsibility, accountability and authority of the NASA CIO in order to drive efficiencies and cost-savings through the acquisition, deployment and management of IT across NASA;
- Using a tool known as Solutions for Enterprise-wide Procurement to help NASA manage a suite of government-wide IT products to meet the requirements of FITARA; and
- Aligning IT and mission strategy in order to achieve goals and measure performance while ensuring stakeholders are informed including:
    - Strengthening the Agency's ability to align IT resources with Agency missions, goals, programmatic priorities and statutory requirements;
    - Clarifying the scope of the Agency CIO's role with respect to program IT and mission IT decisions, as well as allowing the CIO to participate in major Agency decision making processes for Agency missions;
    - Holding the CIO accountable for Agency IT cost, schedule and performance through a new portfolio review process. The CIO will also have new authority and greater visibility into the overall budget planning cycle, allowing me to spot IT resource problems at a mission level earlier on;
    - Increasing transparency of IT resources across the entire Agency; and

- Ensuring that the IT security policies and procedures are implemented at NASA Centers. NASA has recently realigned the reporting structure so that I, as the NASA CIO, have direct authority and oversight over the Center CIOs.

In addition, organizational changes within OCIO are contributing to NASA's improved IT security posture. For example, NASA recently hired its first Senior Cybersecurity Advisor who reports directly to me and serves as my senior technical expert on IT security, staying abreast of the threat environment not only at NASA but also threats to other Federal and non-Government networks that may in turn come to threaten NASA networks. Additionally, I have hired a permanent Chief Information Security Officer (CISO) who serves as NASA's Senior Agency Information Security Officer. She works with all our NASA Center CISOs as well as CISOs across the Federal Government on operational IT security and cybersecurity matters. The NASA Inspector General was correct about the need to have this critical position filled and our new Senior Agency Information Security Officer brings impressive experience and in-depth expertise. Both of these new officials are actively engaged with our Federal partners, thus ensuring that best security practices are implemented at NASA, and that NASA remains coordinated on and protected against threats. They will continue to meet with other Federal IT partners to leverage best practices for IT management and cybersecurity operations.

I am also engaging the private sector for support. While the Federal Government has made significant strides, I know that we do not have all the answers. I am leveraging the expertise of the private sector for advisory and technical services to ensure that our security posture at NASA is benefitting from lessons learned and best practices in the private sector.

NASA IT Threat Environment

Like other Federal agencies, NASA's IT infrastructure is under constant attack from domestic and foreign adversaries. Decades of NASA aeronautics and space technology research and development represents billions of dollars in U.S. Government and aerospace industry investment. The very nature of NASA's mission, and the extremely important technical and intellectual capital produced therein, makes the Agency's information a valuable target for hackers, criminals and foreign enterprises. Many of these threats are well-resourced, highly motivated, and sophisticated. Therefore, there is no perfect, one-size-fits-all tool to predict, counter and mitigate the wide range of attacks across the Federal Government.

The collective actions of NASA's OCIO as well as information sharing with the DHS and other Federal agencies involved in cybersecurity are contributing to an improved security posture. When threats are detected, NASA personnel take immediate action and depending on the level of the threat, NASA alerts other Federal agencies involved with cyber intelligence issues, and partners with them to deter and thwart future attacks. For example, in FY 2015, the NASA Security Operations Center, which is responsible for cyber incident response at NASA, transitioned its incident management process to adhere to the DHS' U.S. Computer Emergency Readiness Team's (US-CERT) new Federal Incident Notification Guidelines[1]. NASA now categorizes all incidents and reports the information at the Federal-level to the US-CERT in near-real-time.

Here are two key metrics that reflect improvements NASA has recently made in its IT security environment:

- NASA has significantly reduced its cybersecurity risk measured by the DHS Cyber Hygiene report. One improved measure of performance, on public facing vulnerabilities, is "time to

[1] OMB Memorandum 15-01, "Updated DHS US-CERT Incident Notification Guidelines", pg. 12-13. October 3, 2014: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

patch." We have looked at the aggregate risk, as measured by DHS, and have reduced our vulnerabilities by 25 percent in the last eight months.

- With regard to NASA's FISMA implementation in FY 2016, we deployed a tool to enable identification of phishing attacks thereby reducing the workload on the end user to identify phishing attacks. For FISMA 2016, we have made inroads on issues such as malware defense and network defense, and we have implemented a secure policy framework on email further reducing the amount of attacks a user would experience.

It is also important to point out that NASA is extremely proactive in our approach for handling breaches caused by human error through awareness and education. NASA reaches out to every employee to notify them of best practices. Employees must take mandatory training in order to retain access to our networks. The Administrator and other senior leaders also have repeatedly stressed to all NASA employees that they will be held accountable for failing to adhere to our established procedures and policies. Additionally, employees are warned before they take any NASA online training, for example, that any misuse of assigned accounts may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

While some Federal agencies, including NASA, have been criticized for our use of legacy IT systems, NASA must sometimes make limited exceptions for the continued use of legacy IT that is critical to the success of long-term Agency missions that were launched, in some cases, decades ago and which are still transmitting data back to NASA. While some IT can be upgraded throughout the project life cycle, a subset of hardware, software applications and operating system components must remain in the state in which they were originally deployed. In these instances, NASA actively monitors all aspects of system end-to-end functionality to assure any IT security risks are identified, contained and mitigated.

Another unique challenge that NASA has in terms of IT security is our statutory mandate to engage the public in our missions and much of that engagement is accomplished via our IT portals. Our Open Data websites, for example, include more than 30,000 publicly-accessible datasets. Therefore, NASA as a whole, and my office in general, must balance securing its IT resources with data accessibility to further global science and technology collaboration around the world.

Work in Progress

Like all agencies, NASA is adjusting to new laws and directives designed to improve how the entire Federal Government improves its IT security posture. While NASA is proud of the progress we have made, we recognize that more work remains to fully comply with new laws and policy. We are making progress with:

- **Patching:** Correcting deficiencies in the timeliness, completeness and tracking of the implementation of security patches is a multi-faceted issue with no simple answer. For mission related software, I, as the CIO, was recently provided additional IT oversight responsibilities within NASA (see enclosure). Additionally, NASA's deployment of the Continuous Diagnostic and Mitigation (CDM) tools will help the OCIO gain better insight into patching vulnerabilities
- **Einstein3A: (E3A):** This capability will allow us to detect malicious traffic targeting NASA networks, but also prevent malicious traffic from harming our networks. As required by DHS, we have worked diligently with DHS and our NASA Centers to deploy E3A. While we have experienced some challenges around deploying this technology at some Centers, we are working with DHS to resolve technical issues and enable NASA to meet the December 18, 2016 deadline for full deployment.

- **CDM:** As required by DHS, NASA's implementation of the CDM program has started with the initial operating phase beginning at our Kennedy Space Center in Florida. This is a necessary step to increase awareness, understanding and effectiveness when we roll CDM out across NASA. The NASA OCIO team has conducted our first lessons-learned evaluation on the CDM deployment at the Kennedy Space Center. We are also partnering with other agencies that have deployed CDM to ensure we have a transfer of knowledge and gain lessons learned from those agencies similar to ours that have already implemented CDM.
- **Incident Response Assessments**: NASA's Incident Response Assessment Program demonstrates our capability to identify, protect from, detect, respond to and recover from issues facing our networks. We conduct assessments once a quarter and identify issues with our NASA-wide enterprise capability as well as those of the individual Centers. We develop process improvements and track those until the issue can be resolved. This is another key check on our processes and systems that assists us as we evolve our security posture.
- **Portfolio Management**: In an effort to strengthen our security posture we are working with the Centers on business cases, for example OMB-300s, to have better insight into their cybersecurity operations. These actions will lead to processes that increase the regular reviews in this area to monitor the risk and progress at an enterprise level. In alignment with FITARA, this increase in accountability will provide more transparency around cybersecurity issues.
- **Authority to Operate (ATO):** We must continuously scrutinize and improve our IT security posture. The security assessment and authorization process is a key element of our overall risk management strategy. To ensure our leadership has the information they need to make truly informed risk decisions, we must provide them a consistent and well understood taxonomy of security requirements, processes, and documentation. In support of this mandatory oversight model, the NASA IT Security Division is deploying a new, modernized toolset (known as RISCS) to more effectively guide processes and capture security assurance artifacts, and to inform NASA senior management on associated cyber security risks. By providing the ATO for a NASA information system, our leadership – myself included – are explicitly accountable to our customers and our missions for ensuring the integrity, confidentiality, and availability of our data. I take this responsibility very seriously. I am working closely with my new Senior Agency Information Security Official to ensure that these expectations are clearly understood, and to make sure that all requisite oversight mechanisms are in place for success.

Conclusion

Protecting and evolving NASA's IT infrastructure is and will remain a top Agency priority.
As evidenced by my testimony today, NASA is fully committed to becoming more secure, effective and resilient, and we are actively pursuing this on all levels. We look forward to working with Congress, the Government Accountability Office, the NASA Inspector General and other Federal stakeholders, including OMB and other Federal agency CIOs and CISOs in effectively implementing a restructured NASA security program.

In conclusion, thank you for the opportunity to testify before you today. I would be happy to answer any questions that you may have.

Enclosure 1

National Aeronautics and Space Administration (NASA)
Business Services Assessment (BSA) Decision Summary
Information Technology (IT) Pilot Deep Dive

Background
In 2015, NASA established the Business Services Assessment (BSA) to strategically assess mission support services, evaluate the health of current mission support capabilities, and identify opportunities to further optimize performance. The NASA BSA supports the Agency's objective of establishing a more effective and efficient operating model to meet current and future mission requirements.

Process
For each BSA activity, NASA establishes a core team, comprised of diverse professionals from across NASA organizations, to evaluate mission support activities. The core teams collect data from across NASA, conduct surveys and interviews with internal stakeholders, review recent audits and regulations, benchmark external organizations, and perform a detailed assessment of existing operations. As part of the BSA process, the Agency employs several feedback mechanisms to collect input from NASA Centers, Mission Directorates, and other key organizations on potential options to enhance the specific mission support activities. Based on the results of the BSA and input collected from across NASA, the Agency makes decisions to strategically re-shape operations in an attempt to optimize mission support services to meet current and future Agency mission needs.

Topic
The Information Technology (IT) assessment was the pilot activity for the NASA BSA. The IT BSA deep dive included assessments of IT roles and responsibilities, governance, data centers, communications, end-user services and security. The findings and decisions below provide a summary of the IT BSA. The Agency Chief Information Officer (CIO) is responsible for oversight of NASA's IT activities, as well as implementing NASA BSA IT decisions.

Findings and Decisions

1. IT Roles & Responsibilities and Governance
Finding: The IT BSA found the existing governance and operating model for IT across the Agency needed to better align with the changing business of IT management and the Federal Information Technology Acquisition Reform Act (FITARA) to ensure compliance with applicable policies, laws and directives as part of the OCIO's responsibility.

Decisions: The OCIO will create a multi-tier (level 0 through level 3) management structure and appoint Program Executives for each IT domain; develop a plan to enable IT management improvements; restructure and streamline existing duplicative IT boards; conduct a formal annual capital investment review as part of the budget process; work with procurement and formalize guidance on strategic sourcing for IT contract activities; and conduct functional reviews of all Centers on a 3-year rotating basis.

2. Data Centers
Finding: The BSA found insufficient strategic direction, consistent coordination and oversight of NASA data center and computing investments.

Decision: The OCIO will implement a federated/hybrid data center operational model by developing an integrated, Agency-wide data center architecture to guide future investments and further consolidation,

including on-site, outsourced, and cloud-based data center services as well as enabling strategic sourcing/contract optimization.

3. Communications
Findings: Multiple NASA Centers were found to have outdated communication services for phones, voicemail and Land Mobile Radios (LMR). In addition, the deep dive found that some mission areas were unable to effectively and securely collaborate using existing IT infrastructure.

Decision: The Agency will realign NASA Integrated Communications Services (NICS)-provided voice services, network operations and transformation funding from Centers to the Agency OCIO to enable an enterprise funded and managed approach for communications.

4. End-User Services (Workstations and Collaboration & Content Management Tools)
Findings: The Agency Consolidated End-User Services contract (ACES) was not being used as extensively as intended, which led to less than optimal IT operations. The deep dive also found multiple contracts and methods were being used to procure and administer workstations; and numerous independent platforms and tools were being used across NASA for collaboration.

Decisions: The OCIO will consolidate Non-ACES workstations administration and support, where feasible and appropriate. A target was established for each NASA Center to obtain at least 80% of their desktop, laptop, and workstation computing services through ACES. Further, the Agency decided that using non-ACES systems would require waiver approval from the Center CIO. Compliance with these objectives will be evaluated as part of the annual Center functional reviews. Finally, the OCIO will develop a core suite of collaboration tools and standards to meet the majority of NASA requirements.

5. IT Security
Finding: The absence of an enterprise-wide risk management framework created gaps managing NASA's cybersecurity risks, implementing the Agency's cybersecurity program, and effectively managing cybersecurity resources and tools.

Decisions: The OCIO will sponsor a zero-based review of IT Security spending and ensure alignment to the NASA IT security strategy. The OCIO will also establish an Agency IT Security risk management framework and IT security architecture that aligns with NASA's business risks.

Mr. HURD. Thank you for your remarks, Ms. Wynn. And thanks for being here again.

Mr. Alboum, you're recognized now for 5 minutes for your opening remarks.

STATEMENT OF JONATHAN ALBOUM

Mr. ALBOUM. Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, thank you for your diligent work on cybersecurity and the IT scorecard. I appreciate having this opportunity to share USDA's efforts to strengthen its cybersecurity posture over the last few years.

The Department of Agriculture touches the lives of all Americans. Protecting USDA customer, partner, and employee data is a top priority for Secretary Vilsack and me. Together, we work across USDA to ensure we have the right tools and culture as new threats emerge. In terms of cybersecurity tools, I'm pleased to tell the committee that USDA has successfully completed our initial implementation of EINSTEIN 3A. USDA employs a risk-based approach to cybersecurity, prioritizing resources where they will have the most significant impact. EINSTEIN is key to this approach. Over the coming weeks, we will continue to work with DHS to bring additional EINSTEIN capabilities online. And we fully expect to meet all of the December deadlines.

I'm also proud to share that USDA is one of the leading agencies participating in the DHS continuous diagnostic and mitigation program, also known as CDM. I've made this a priority for the Department. We are currently implementing the capabilities of phase 1, which gives us increased insight into what is on our network. This improved visibility helps us to prioritize future modernization initiatives and protect the information of the people we serve. EINSTEIN and CDM, combined with our security operation center, or SOC, position USDA to proactively detect, prevent, and mitigate cyber attacks. The USDA SOC is starting to use big data technologies to analyze trends and anomalies by correlating security data from multiple sources. We have partnered with the Defense Advanced Research Projects Agency, DARPA, to pilot many of these tools. As pilots like these demonstrate positive results, USDA will explore the potential for a departmentwide rollout.

Additionally, my team routinely conducts penetration testing assessments to identify security vulnerabilities in our systems. These findings are used to develop plans to remediate risk and improve system security.

USDA also created a list of high-value assets and has worked with DHS to perform additional penetration testing assessments of these systems over the past year.

Effective cybersecurity is as much about education and culture as it is about having the right tools in place. Secretary Vilsack strongly supports my office in ensuring that USDA senior executives and employees understand their daily role in preserving the Department's reputation as a trusted government partner.

In the past year, I created scorecard to build awareness of the Department's cybersecurity posture. Every 2 weeks, component agency heads are provided with a status of key cybersecurity hygiene factors for their organizations. This increased insight gives

USDA officials the information they need to balance programmatic requirements with continuous improvements in cybersecurity. For example, this approach supported our drive to increase the usage of personal identity verification, or PIV, cards across the department. Over the past 16 months, we increased our usage rate from 15 percent to over 92 percent for nonprivileged users and from 6 percent to over 96 percent for privileged users.

USDA employees face an increasing number of malicious emails and social engineering cyber attacks like phishing. Through a recent anti-phishing campaign, we recognized that additional safeguards, like email subject-line warning messages, were needed to render phishing attacks less effective. As a result of these activities, USDA achieved a greater than 50 percent reduction in the click rate of simulated phishing attempts. Further, my team and I fully support the push for additional measures to improve information sharing across government to enhance cybersecurity readiness and response. In May 2016, USDA became the first department to develop and successfully test new procedures required by the Federal Cybersecurity Enhancement Act for notifying Congress within 7 days of a major incident.

As threats continue to proliferate and to adapt to existing defenses, USDA, like all government agencies, will need appropriate resources to employ emerging technologies and new approaches to mitigate these risks. For example, the Department's fiscal year 2017 budget included a requested increase of $10 million to enhance USDA cybersecurity capabilities. It is critically important that we discuss these issues and related impacts.

So, again, I want to thank you for holding this hearing to shed light on this important topic. I'm grateful for the opportunity to share information about our progress in strengthening USDA's cybersecurity program. USDA is committed to an open and continuous dialogue with Congress about new opportunities to improve our defenses. I look forward to your questions. Thank you.

[Prepared statement of Mr. Alboum follows:]

Statement by
Jonathan Alboum
USDA Chief Information Officer
Before the Committee on Oversight and Government Reform
Subcommittee on Information Technology
U.S. House of Representatives
November 16, 2016

Chairman Hurd, Ranking Member Kelly and Members of the Subcommittee, thank you for your diligent work on Cyber Security and the IT Scorecard. I appreciate having this opportunity to share USDA's efforts to strengthen its cybersecurity posture over the last few years.

The Department of Agriculture touches the lives of all Americans. Protecting USDA customer, partner, and employee data is a top priority for Secretary Vilsack and me. Together, we work across USDA to ensure we have the right tools and culture to meet new threats as they emerge.

In terms of cybersecurity tools, I'm pleased to tell the committee that USDA has successfully completed our initial implementation of Einstein 3A. USDA employs a risk-based approach to cybersecurity, prioritizing resources where they will have the most significant impact. Einstein is key to this approach. Over the coming weeks we will continue to work with DHS to bring additional Einstein capabilities online. We fully expect to meet all of the December deadlines.

I'm also proud to share that USDA is one of the leading agencies participating in the DHS Continuous Diagnostics and Mitigation program, also known as CDM. I've made this a priority for the Department. We are currently implementing the capabilities of Phase 1, which give us increased insight into what is on our network. This improved visibility helps us prioritize future modernization initiatives and protect the information of the people we serve.

Einstein and CDM, combined with our Security Operations Center (SOC), position USDA to proactively detect, prevent, and mitigate cyberattacks. The USDA SOC is starting to use "Big Data" technologies to analyze trends and anomalies by correlating security data from multiple sources. We have partnered with Defense Advanced Research Projects Agency (DARPA) to pilot many of these tools. As pilots

like these demonstrate positive results, USDA will explore the potential for Department-wide rollout.

Further, my team routinely conducts penetration testing assessments to identify security vulnerabilities in our systems. The findings are used to develop plans that remediate risks and improve system security. USDA also created a list of High Value Assets and has worked with DHS to perform additional penetration testing assessments of these systems over the past year.

Effective cybersecurity is as much about education and culture as it is about having the right tools in place. Secretary Vilsack strongly supports my office in ensuring that USDA's senior executives and employees understand their daily role in preserving the Department's reputation as a trusted government partner.

In the past year, USDA created a scorecard to build awareness of the Department's cyber security posture. Every two weeks, component agency heads are provided with a status of key cybersecurity hygiene factors for their organizations. This increased insight gives USDA officials the information they need to balance programmatic requirements with continuous improvements in cybersecurity. For example, this approach supported our drive to increase the usage of Personal Identity Verification (PIV) cards across the Department. Over the past 16 months, we increased our usage rate from 15% to over 92% for non-privileged users and from 6% to over 96% for privileged users.

USDA employees face an increasing number of malicious emails and social engineering cyberattacks, like phishing. Through an anti-phishing campaign in 2016, we recognized that additional safeguards, like email subject line warning messages, were needed to render phishing attacks less effective. As a result of these activities, USDA achieved a greater than 50% reduction in the click rate of simulated phishing attempts which further reduces Departmental vulnerabilities to such cyberattacks.

Further, my team and I fully support the push for additional measures to improve information sharing across Government to enhance cybersecurity readiness and response. In May 2016, USDA became the first Department to develop and successfully test new procedures required by the Federal Cybersecurity Enhancement Act for notifying Congress within 7 days of a Major Incident.

As threats continue to proliferate and to adapt to existing defenses, USDA, like all Government agencies, will need appropriate resources to employ emerging technologies and new approaches to mitigate these risks. For instance, the Department's FY 2017 Budget included a requested increase of $10 million to enhance USDA's cyber security capabilities. It is critically important that we discuss these issues and related impacts. So, again, I want to thank you for holding this hearing to shed light on this important topic. I am grateful for the opportunity to share information about our progress in strengthening USDA's cybersecurity program. We are committed to an open and continuous dialogue with Congress about new opportunities to improve our defenses, and I look forward to your questions.

Mr. HURD. Thank you, sir.

Mr. Klopp, you're on the clock for 5 minutes. We welcome your opening remarks.

STATEMENT OF ROBERT KLOPP

Mr. KLOPP. Thank you. Good morning, Chairman Hurd and Ranking Member Kelly.

Earlier I provided a status update in my written testimony, which I won't repeat here. But I would like to share a couple of updates, provide a review of our Department of Homeland Security reporting, and share some thoughts tied to the OPM breach report.

First regarding the status of our EINSTEIN implementation, the agency completed phase 3 of this program in March of this year. And it's been in production since then. So we were early.

Next, regarding our implementation CDM, which has been mentioned here, we're on schedule to deploy phase one of that in December. So we're on track there as well.

Now, I want to talk a little bit about some of the ongoing Department of Homeland Security reporting. What we see is sort of a continuous process of discovery and remediation. DHS has come onsite twice to evaluate high-value assets. This resulted in 16 recommendations. They called out two critical items, one of which was a vulnerability. Eight of these items are resolved, including both critical items. Five recommendations are complete but require sort of continuous improvement. Two are in progress and were resolved in this fiscal year. And one around network segmentation is actually a very large project which we'll begin in fiscal year 2017.

As you may know, the DHS scans the agency weekly, producing cyber hygiene reports. I'm happy to report that it found no critical vulnerabilities since the inception of this program.

DHS also produces monthly vulnerability reports. This process sort of continuously reports that we score in the top three, with the smallest number of vulnerabilities of any reporting agency.

Proactively the agency runs daily inhouse penetration tests managed through an automated system. In 2016, we identified 1,872 vulnerabilities and remediated them on the average of every 22 days.

The agency participates in an annual financial statement audit. In fiscal year 2015, auditors found no material weaknesses, one significant deficiency, and produced 59 findings and recommendations. Since these findings, we have implemented automated support to request new access to systems to schedule the removal of access for departing staff and progressed in all but one of the 59 findings.

Most importantly, I'm happy to report that the agency has no major incidents to report to date.

Regarding the OPM breach report, we took this report very seriously. In the interest of time, let me sort of focus on what we think is the most far reaching of the 10 recommendations. That was recommendation No. 2 regarding the deployment of a zero-trust model. I'd like to give you sort of an example of our intention and direction on that. We are implementing now a new zero-trust capability for systems administrators where access is revoked and renewed with each new administrative task. These administrators don't get any permanent passwords. As you may know, systems ad-

ministrators hold the keys to the kingdom. By implementing a zero-trust model for sys admins, first, we expect to significantly upgrade our posture.

I think all of the, you know, witnesses here are testifying about the increased threat of cyber attack. It's not a surprise. And some are suggesting that we need to take a more aggressive stance as a government with regard to that. But I think our IT systems are sort of the equivalent of B–52s: dependable, but outdated and vulnerable. We appreciate this committee's awareness of the need for IT modernization and appreciate even more the bipartisan measure, H.R. 6004, which you mentioned. It's a really important step. But H.R. 6004 is an unfunded vehicle. And what we need is funding. To defend our IT assets to the standard you and the public expect, we need the cyber equivalent of defense spending. And we need a fully funded investment in IT modernization.

So I'd like to thank you for your support. And now I'm happy to take any questions you might have.

[Prepared statement of Mr. Klopp follows:]

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON INFORMATION TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

November 16, 2016

STATEMENT FOR THE RECORD

ROBERT KLOPP
DEPUTY COMMISSIONER OF SYSTEMS
CHIEF INFORMATION OFFICER
SOCIAL SECURITY ADMINISTRATION

Chairman Hurd and Ranking Member Kelly, thank you for inviting me to testify today to discuss cybersecurity at the Social Security Administration (SSA).

In this testimony I will provide you with an update that describes our progress and open issues related to the external audits of our cybersecurity program; I will provide you with an update related to other projects that have resulted from our own examination of our systems; and I will provide you with a status of our efforts to protect personal information.

I would like to suggest one issue on-the-record for consideration by the Committee. The Council of Inspectors General has established a measurement standard for compliance with the Federal Information Security Management Act (FISMA) Information Technology (IT) Security guidelines. Unfortunately, the standard has changed significantly each of the past three years and, as a result, one cannot judge progress against a standard set of criteria. In FY 2015, the Inspectors General (IGs) introduced a maturity model for Information Security Continuous Monitoring, which, as stated in the Office of Management and Budget's (OMB) Annual Report to Congress, led to a decrease in overall agencies scores. In FY 2016, the IGs introduced a second maturity model for Incident Response, which will likely lead to a further decrease in scoring due to the scoring methodology. The maturity model provides agencies with context for performing risk assessments and identifying the optimal maturity level that achieves cost-effective security based on their missions and risks. The IGs indicate that they plan to coordinate with the Department of Homeland Security (DHS), OMB, and other key stakeholders, and extend the maturity model to other security domains for IGs to utilize in their FY 2017 FISMA reviews. In the meantime, however, metrics for those domains without an established maturity model are mapped to Maturity Model Indicators. These indicators will act as a stepping-stone, allowing IGs to reach preliminary conclusions similar to those achievable with a fully developed model

We will continue to work with our Inspector General to address deficiencies across these areas.

To that end, the SSA cybersecurity team is recognized as one of the better teams in the federal government. As I describe in my testimony, we have made significant strides forward since our last visit before this Committee in May.

In our last hearing, some Members voiced concerns about a lack of leadership on cybersecurity at the agency. I appreciate this concern, but I also think we need to be careful about assuming that any security weakness is the result of bad management. If the fact that there are vulnerabilities in our IT infrastructure reflects a lack of leadership, then I accept the responsibility for the lack of leadership. If the criteria is that, if DHS finds anything wrong, this reflects a lack of leadership, then I accept the responsibility. But this also means that every agency that has a vulnerability, exploited or not, has a leadership issue – and that means every agency, not just SSA.

The cost of continuously deploying ever better cybersecurity is growing with the many threats from bad actors. The ability to protect legacy systems becomes more difficult as modern cyber defenses are not built to protect 30-year-old systems.

The SSA can shift funding from our IT budget for cyber, but soaking up any savings by spending it on cyber does not fund continuous improvement. It does not fund IT modernization. The idea that the SSA, or any agency, can do more in cyber while simultaneously rebuilding our IT infrastructure is no less a fantasy than the idea that the country can modernize any other infrastructure – our roads, our dams, our electric grid, our military – without an investment.

My testimony includes a request to modernize IT and to fund improvements in cyber defenses. Wishing for better IT from cost cutting will not help. Wishing for cost-cuts with no investment will not help. Passing legislation without providing funding is not enough.

In the remainder of this testimony, I will outline the issues and remediation undertaken by my cybersecurity staff since our last hearing.

OIG FISMA Audit

In 2015, the Office of the Inspector General (OIG) FISMA Audit identified several areas where the agency needed to improve our program.

In FY 2016, we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources.

It was noted that we needed to improve our application of the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) requirements for our remote locations: regional offices, program service centers, and Disability Determination Service systems. This is a significant undertaking.

During Fiscal Year (FY) 2016, we established a security assessment and authorization process that resulted in providing authority to operate (ATO) for 221 software applications in our regional offices and program service centers. This regional ATO process builds on our mature and robust RMF process for our centralized systems. We also improved our system inventory management process by expanding the use of an automated inventory software to capture details about applications housed remotely. We have not closed this issue but we are making significant progress.

We conducted a review of our national teleservice center system hosted by AT&T. After directing the vendor to make a series of changes, we granted an ATO. We conducted security reviews of other external contractor-operated systems using the same NIST processes we use for our internal systems. We include contractor systems in our automated inventory.

Auditors noted room to improve our access controls in order to prevent unauthorized access to our systems and data.

In FY 2016, we implemented an automated Security Access Management portal solution to replace our paper-based access request and approval process and established an authoritative database for contractor access. We implemented a Security Administration Reports Application and began the implementation of an automated Access Removal Tool for terminating or disabling logical and physical access for separated employees and/or contractors.

We expanded our user account review process to increase our focus on privileged user accounts and procured a new technical solution to further strengthen and automate management over our privileged user accounts.

We updated our security and privacy training to reflect the current threat landscape. Nearly 85,000 of our employees and contractors completed our annual training that covered a range of topics including protection of sensitive data, such as personally identifiable information, and how to prevent, detect, and report security incidents or suspected incidents when they occur. Additionally, we conducted ongoing training exercises to test our users' ability to detect social engineering attacks such as email phishing.

The auditor cited a weakness in tracking completion of security awareness training for all contractors.

We previously noted the establishment in FY 2016 of a contractor database. This database will log contractors' completion of mandatory security and privacy awareness training.

Audits suggested that we needed to continue improving our threat and vulnerability management process.

In FY 2016, we expanded our enterprise-wide penetration-testing program and implemented new tools to improve our detection of potential vulnerabilities across our network. This implementation has allowed us to find certain security threats in near real time.

The auditor cited a weakness that SSA had not implemented plans to close Information Security Continuous Monitoring skill gaps, knowledge, and required resources.

We began working with DHS under their Continuous-Monitoring-as-a-Service phase of the Continuous Diagnostics and Mitigation (CDM) program, which will allow us to feed information automatically about our asset, configuration and vulnerability posture directly to DHS to feed the federal dashboard, thereby improving visibility into all federal agencies. It also provides us with new capabilities to prevent unauthorized software on our network. While we have trained staff with the necessary skills and resources to meet all CDM program requirements, we face challenges similar to all Federal agencies in attracting and retaining cybersecurity talent.

DHS Cyber Exercises

We participated in several exercises where DHS staff were allowed access to our systems to find issues. There are several recommendations resulting from these exercises.

We have created a regimen that allows both DHS and our cyber staff to scan the mainframe environment regularly for vulnerabilities. Our regularly scheduled scans have found no significant issues there to date.

In addition, at our last hearing before HOGR it was pointed out that we needed to change the process where we notified OIG of a DHS exercise but waited for a formal request from them for

the results, to a process where we automatically shared results after each exercise. We have done so.

FITARA Scorecard

In the May 2015 Federal Information Technology Acquisition Reform Act (FITARA) scorecard the agency received an overall grade of "C." Although we received high grades in some categories, we received "F"s in two categories.

We received an "F" for "Incremental Development." Our efforts to reduce time and increase the number of times we deliver product increments is paying off. In addition, we are actively pushing Agile development methods in order to improve further our ability to develop software faster and cheaper.

We also received an "F" for "Data Center Consolidation." Since our last hearing, we have finished the development and deployment of our Urbana data center. Recently, your staff toured the facility and, it is my understanding, they came away impressed. With the closure of this project, the agency is fully consolidated and runs only two data centers: a primary and a back-up. This should improve our grade to an "A," fully consolidated.

We believe that these two improvements would push our overall grade to a "B" if the criteria were to stay the same.

Internal Projects and Status

This topic provides an overview of capabilities-in-place and of other projects unrelated to external parties.

General Notes

The agency is incubating a series on modern IT capabilities in preparation for a series of funded IT modernization programs. Each of these new technologies goes through a comprehensive review before receiving an ATO.

Cloud Computing

We utilize the General Services Administration's Federal Risk and Authorization Management (FedRAMP) program to guide the security of our cloud-based systems. In FY 2016, we issued our first provisional cloud ATO for our Agency Cloud Infrastructure platform as a service.

Enterprise Data Warehouse

We are deploying new Open Source technologies as part of the first agency-wide decision support/ Enterprise Data Warehouse product. These technologies build upon the ATO for cloud computing and this new platform has received authorization to operate.

Identity Assurance for Public Facing Applications

The agency is planning to implement methods that adhere to the NIST Identity Assurance Level 3, when providing a citizen access to our online services.

This fall, the agency moved to improve our ability to authenticate users with existing IDs by implementing a technique called multi-factor authentication (MFA). Our implementation of Multi-factor authentication requires users to respond to a prompt sent to a device in their possession.

Unfortunately, our implementation created a security barrier that some citizens could not overcome so we backed out MFA and immediately began designing a new MFA approach that would implement secondary factors that allow any computer user to login. We expect this new protection to be deployed in the first half of calendar 2017.

Incident Response

We have a comprehensive Incident Response process in place. We prepare, plan and conduct Incident Response testing every six months. Our testing in FY 2016 included establishing a process to fund our recovery in the event of a large-scale breach. We also have an automated capability to report personally identifiable information losses and incidents detected by our Security Operations Center to DHS' United States Computer Emergency Readiness Team (US-CERT) within the required timeframes.

We perform a range of agency-wide activities designed to identify threats to our agency mission and operations, and plan for the recovery of IT assets needed to support our essential functions. We have established Continuity of Operations Plans (COOP) at the agency and component levels, which identify our mission essential functions. We have conducted a Business Impact Analysis to determine the potential adverse impact that the loss of our IT infrastructure would have on our ability to perform essential functions. We have further developed a Disaster Recovery plan that provides for full redundancy of our major systems. We conduct annual COOP testing and disaster recovery exercises that test the recovery of our major systems.

IT Modernization

I would like to emphasize that we also need to modernize our legacy systems to provide the modern infrastructure that incorporates modern cyber defenses. 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. The Administration's proposal for the IT Modernization Fund would provide an additional opportunity to secure much needed IT modernization funding.

To that end, 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 long-term investment in several areas including modernization in computer languages, databases, and infrastructure.

We need this additional IT modernization funding because our annual funding levels have been insufficient to undertake this important IT work. We are working hard to manage the agency with far less money than we need. Our FY 2016 enacted budget was around $350 million less than the President's Budget request. As a result, we are seeing service degradation in many areas. SSA's core operating budget has shrunk by 10 percent since FY 2010 after adjusting for inflation, while the number of Social Security beneficiaries rose by 12 percent over the same period. We are greatly concerned about FY 2017, when we will serve a record number of beneficiaries, at a time when people are already facing longer wait times for service in our frontline offices.

Each year, over $300 million of our budget represents fixed cost growth for things such as increases in salaries, benefits, rent for our buildings, and guard costs. The continuing resolution (CR) leaves us with few resources to improve overall service. With services already in a fragile state, it is critical that we receive sufficient funding when Congress passes a full-year budget for FY 2017 – and it is critical to receive adequate funding to carry out IT modernization to protect the public's data and enhance service to the public. The FY 2017 President's Budget request of $13.067 billion is necessary to rebound from this year's constraints, to improve service to the public, to maintain service hours to the public in our offices, and to begin the needed work to protect and modernize our IT infrastructure. I would be happy to have our budget office brief you or your staff in greater detail.

Conclusion

Thank you for holding this hearing. I would be pleased to answer any questions you may have.

Mr. HURD. Thank you, sir.

And I'll recognize myself for 5 minutes.

Ms. Wynn, when did you start in your position?

Ms. WYNN. I started with NASA on July 13 in 2015. And I became the chief—I started as the deputy CIO, and I became the chief information officer at the end of September of 2015.

Mr. HURD. Gotcha. So if my math is correct, about a year? A little bit under?

Ms. WYNN. Just slightly over a year, going toward 14 months.

Mr. HURD. So I guess we're in November now.

There's been plenty of reports about how, over the summer, NASA's—the Agency Consolidated End-user Service, or do you call it ACES—yeah—was operating under a conditional authority to operate since July 24. My understanding is that you declined to sign off on the authority to operate for ACES because of a difference of opinion between your office and the contractor operating the system. That—the issue was over patching, it seems like. Now, I think this is a—actually a good news story, right? Because you obviously felt you had the authorities to do those kinds of things, and you're using your technical judgement.

Can you walk us through the thought process during that decision?

Ms. WYNN. Yes.

Mr. CONNOLLY. Would my friend yield just for a second?

Mr. HURD. Sure.

Mr. CONNOLLY. Forgive me, but I have a hearing upstairs, but I didn't want to miss this. I just ask unanimous consent my opening statement be entered into the record. Forgive me, I've got to go back upstairs to another hearing on the census. But someday hopefully the good Lord will give me the gift of bilocation.

Thank you, Mr. Chairman.

Mr. HURD. Without objection. Thank you.

Mr. HURD. Ms. Wynn.

Ms. WYNN. NASA will get to work on that bilocation.

Yes. So, yes, the authority to operate for our end-user services, we have several of them. It's a very complex set of systems. The one in particular had to do with the client-based devices that we use, computers and that. And it was presented to me on July 25. The presentation is on the security risks and how those risks were being—to be mitigated. And upon that, I asked if they can look me in the eye and say free and clearly they would recommend signature. And on that date, they presented to me the package as we usually go through. And at that point, both on the operational side as well as the gentleman who was brought in for security to serve as the acting acting CISO as our acting CISO was on vacation, on the operational side recommended—said that they could not recommend to me signature because we had a discrepancy on numbers of devices as well as the status of the patches and how quickly they were being deployed and the status of that deployment. So it was both a timing and an end effort. And the gentleman who was acting as the acting acting CISO for me at the time said that he also could not agree to—could not recommend signature for the authority to operate. And so I asked a series of questions. What does that really mean? And in this instance, we didn't have enough data

to make a sufficient risk determination on whether the ATO should be signed or not. And so, at that point, I said that I would not sign and that work needed to be done on the side of both NASA as well as HPES to get the work done. By that Friday—so this was a Monday—by that Friday, I had signed the authority to operate because we were able to see and understand the risks that I would be signing off on.

Mr. HURD. So did that give anyone at NASA heartburn? Did you receive any flack for not signing off on an ATO? Because if I remember correctly, the news coverage at the time—I think the term was "unprecedented step." And I imagine that a CIO letting a major system authorization to operate expire turned some heads.

Ms. WYNN. Yes, Chairman, it did turn some heads. So the actions rate when one does this action, news of this significance would spread fast. So I made sure that the chief information security officers around our centers, as well as our chief information officers around the centers, were aware of my decision. And then my next step was to inform the Administrator and the Deputy Administrator of the action that I had taken, as well as letting our press office know, as well we figured that there would be—this would leak out and become information and headlines. And so I was supported by everybody for making this decision. And I would do it again. I wish that we hadn't ever reached that point. And so we worked on some prevention efforts. HPES has definitely stepped up to the plate in terms of working with us. And they and my team have actually responded very positively that the authorities to operate, as you said, are not to be rubber-stamped. If my signature's on that and there had been a breach the next day, then it would be very obvious that I would not have done the job that I was asked to do on behalf of the NASA as well as the Federal Government.

Mr. HURD. Well, I'd like to commend you on making a tough decision. And these are the kinds of decisions that we want to see more CIOs making. That's the whole reason we're empowering you to make these types of decisions.

So I'd like to answer a procurement question a little here. And so if a system doesn't get the approved ATO, how does that work? You know, does that—do you have the authority to change, move? Does that void the contract? How does that—can you give me some insight onto that process?

Ms. WYNN. NASA's procurement for an information system has the security requirements—the Federal security requirements in that I am—we would need to work on procurement clauses, and I think these would need to be broad Federal Government clauses, in terms of ramifications of an authority to operate and what would happen after that. The CIO, in concert with the rest of the agency, would need to be able to work out whether that system needed to be shut down and modernized or upgraded or—because not every system is the same. Others are not in a clean position to say, "Okay, we just can't do this anymore," and go that. So we would need some flexibilities to make those determinations. But I believe that procurement clauses would need to be added for the benefit of the Federal Government.

Mr. HURD. So am I understanding your statement correctly, you would like to have that authority?

Ms. WYNN. I would like to have that authority.

Mr. HURD. Mr. Alboum, do you have any opinions on this topic on ATOs and budget authorities and things?

Mr. ALBOUM. Sure. Thank you, sir. So, in the year or so that I've been the USDA CIO, I have not been in a situation where I've had to disapprove an ATO or not sign. However, similar to Ms. Wynn, I see within the U.S. Department of Agriculture the support to make the right decisions. We have an enterprise IT board that we're able—that is composed of our Under Secretaries, Chairman, the Deputy Secretary, where we can bring challenging IT decisions before that board and have a robust conversation. So we have done that. Not on an ATO, however.

On the point regarding procurements, having that contract language, I think, would be very good, and I agree that it would need to be something that's government-wide. We'd have to understand how that works, as oftentimes, with the establishment of an ATO, there's a component that is—the contractor's required to do. There's a component that the Federal staff has to do. So having good very clear roles and responsibilities and very clear timelines would be critical. Procurement language—contract language would definitely help.

Mr. HURD. Mr. Klopp, any opinions on this?

Mr. KLOPP. Actually, we had a very similar situation to the NASA situation where we had a very large contractor who was running our call center and how—was not compliant. We took a little bit different approach, which was that we revoked the permanent ATO and provided them with a provisional ATO that extended for 90 days, and then continued to extend that and put pressure on them threatening the unprecedented move that Renee went to, but never actually pulling the trigger on it. In the end, it took us about a year to get that system completely compliant. But the pressure and threat of pulling the ATO is what allowed us to do it. So I would probably—I mean, I would certainly agree if we were able to have the kind of—some sort of legal wording in there that forced venders to do this as one more lever on top of them, that would be really valuable for us.

Mr. HURD. Because I would even take it a step further and, you know, in the MGT Bill, when we get that passed the Senate—Senate, I hope you're listening—this is an opportunity—because if you had to change, if you had to move in a different direction, I would consider that savings. All right? That is, if some project had to stop, I would consider that savings and would be able to go into the working capital fund that you would continue to have access to for 3 years, right? So that is an additional tool so that you're not having to run against the clock. And I think what most people don't recognize is that your systems, your networks, are so big and there's so many devices on it that changing a system in the course of a year is next to impossible. And that's why you need the additional flexibilities with those resources. And so that would be the next logical continuation of this topic.

Ms. Wynn, the ACES, is it currently operating on a conditional or has it gotten a standard ATO?

Ms. WYNN. Our ACES contract is on an ATO that, like Rob was talking about, that's running on an 18-month timeframe. So—and we've got regular meetings on both the ATO as well as making sure that our teams, NASA and HPES, are working together to ensure that the next ATO is either longer or has the right timeframe for checks and balances.

Mr. HURD. And, Mr. Alboum, am I to infer from your statements that USDA does not currently have any systems operating without an ATO?

Mr. ALBOUM. No. That's not correct. There are some systems that don't have an ATO. USDA's employed an ongoing assessment process. And we assess one-third of all of the controls of each system—we have 329 systems—annually. So it is possible, during the assessment of those controls, we will find something that requires us to revoke an ATO and work with an agency to get back into compliance. So the number of systems we have and the number of systems that have a valid ATO is in flux because of this process. So, again, to your point, I think it's a good thing if we find something that says we're not going to have an ATO for this system right now. We're going to work to correct it.

Mr. HURD. Gotcha. Thank you.

I'd like to now recognize Ms. Kelly for her lines of questioning.

Ms. KELLY. Thank you, Mr. Chair.

I wanted to dig a little deeper into the cyber requirements for government contractors. In my opening statement, I mentioned that the minority staff of this committee found that Federal cybersecurity is intertwined with government contractors and that cyber requirements for government contractors are inadequate. So, in response, OPM has strengthened its contracting requirements by heightening incidence reporting and access to contractors' systems.

Ms. Wynn, would you agree that having increased incident reporting requirements and access to contractor systems will enhance Federal cybersecurity? And if you agree, how so?

Ms. WYNN. Congresswoman, the answer is yes.

Ms. KELLY. And do you have similar requirements for contractors at NASA?

Ms. WYNN. We have the—a lot of the standard clauses required to pass along the Federal requirements onto those contractors, and we work to enforce those as well.

Ms. KELLY. Okay. And has NASA taken any other measures regarding cybersecurity in the wake of the OPM breach?

Ms. WYNN. Yes, we have. We've done a couple of efforts. One is, is that, at NASA, given some of the sensitive work that we do and intellectual property that we have, we are definitely a target for hackers. And so we've got a number of—not getting too technical, but we've got air gap systems. We take a look at what our high-value assets are. In fact, we're working right now to trim the list of high-value assets so that it's a single list for the agency, instead of one from a cyber perspective and another for safety. Because safety and cyber go hand in glove for NASA, as they would probably for any Federal agency. And we—with our new Federal CISO, we're also taking a hard look—not Federal CISO. She works NASA. Sorry. She's taking a hard look at our processes and procedures and making sure that we are in fact doing the best that we can

do with tools and bringing in assistance from other Federal agencies.

Ms. KELLY. Thank you. And our other witnesses, have your agencies done anything to enhance the cybersecurity—cyber requirements for contractors in response to the breach?

Mr. ALBOUM. Yeah. So we have an incident response policy as USDA that contractors are required to follow if they're to lose personally identifiable information or sensitive but unclassified kinds of information. So that is something that USDA contractors are required to follow.

Mr. KLOPP. Yeah, I would say sort of two things. One is SSA's really a little bit different than most other agencies in that 75 percent of the work we do in the agency is done with Feds instead of with contractors. So it's a little bit less of a problem for us. But it's—the problem is still there.

I would say two things that we've done that are critically important. One is we've just upgraded the sort of automated support we have for managing contractors and—which means that it makes it—there's a more automated mechanism for us to make sure that when a contractor rotates out, that we instantly take away all access they have to the systems. That is really significant. We were having problems where people would leave, the contractor wouldn't notify us, and they might have retained access for some period of time. So I think we've got that fixed.

The second thing I would go back to is this sort of, you know, zero-trust rule. What we're doing now is, by implementing this new system that allows systems administrators to really have to renew a password every time they take on a task, it basically allows us to give administrative rights to contractors knowing that those rights will disappear within a day.

Ms. KELLY. Is there a breadth or are there a breadth of contractors that you can use? Or is it the same people all the time, the same contractors? Or do you have a lot of options, do you feel?

Mr. KLOPP. Well, I mean, I think that there are, you know, what we refer to affectionately as the "cartel." Right? So there's a bunch of big ones. But one of the things I think is really an exciting new trend going on that was sort of driven by the GSA 18F folks and by the U.S. Digital Services folks is the idea of allowing us access through contracting vehicles to smaller, more niche contracting agencies that have a really different kind of a profile and a different attitude as well. And so those things will, I think, improve the quality of some of the contractors we get at the cost of having some administrative issues because we'll be dealing with more companies.

Ms. KELLY. Do you have any response?

Ms. WYNN. Yeah. So NASA does have a lot of contractors, and we have a lot of partnerships, different types of partnerships, with the private sector as well as academics and a lot of work with the public. And so we use some of the bigger contractors. We use some of the smaller contractors. We try to make sure that we give a lot of opportunities to our small businesses. So, on the backside of that, it means you're going to have to have a lot of smart folks to be integrators, either whether it's within the contracting community integration and ensuring that they're collaborating and cooper-

ating. The other side is they bring systems to the table as well. And so you also have to make sure that you've got really good systems integration. And so NASA is pretty accustomed to systems integration. And so for us to have a whole breadth of contractors and their capabilities and what they work on allows us to then be in a pretty good position in terms of managing those differences. Because every time you add a contract, you had overhead and responsibility on the Federal Government side. And you've got to be good at that for that to be—to work for you.

Ms. KELLY. Any comment? It's up to you. You don't have to.

Mr. ALBOUM. No. Sure. I think what's been said is very accurate. The government is going to rely on contractors to do particular tasks and support work. And the idea of having competition and having healthy competition between companies is the way we want USDA to operate. We don't want to be locked into vendors. The idea that some venders come into the government, and they feel, "Well, they'll always be here," we're working very hard to change that. That sort of mentality breeds the opportunity for people to feel—sometimes the contractors to feel like they are employees and to take liberties or to maybe think, "Well, these rules don't apply to us." So we want to make sure that all of our venders that we rely on and have good relationships with recognize that they're there to do a particular job, that we will re-compete that work as appropriate, and there are no guarantees that they will remain in position to continue to do that work if they don't do a good job, if we don't think that they're following appropriate security protocols, they don't respect the environment that they're operating within.

Ms. KELLY. Thank you. I yield back.

Mr. HURD. Thank you.

And now I'd like to recognize the distinguished gentleman from Iowa, Mr. Blum, for his remarks and questions.

Mr. BLUM. Thank you, Chairman Hurd.

I'd like to welcome the witnesses today. Thank you very much for being here, imparting your wisdom on us. I'd like to talk specifically about the Social Security system, Mr.—it's Klopp, correct? The Disability Case Processing System. I understand, in 2008, we undertook a very large project to consolidate I think it was 54 fragmented custom systems, which we see a lot of this across government, and this is good to get rid of these customized fragmented systems into one system. I also understand we've spent, to date, over $400 million on this project. I'm from Iowa. And in Iowa, $400 million is a lot of money.

So, first of all, Mr. Klopp, I'd like to have you give me an update on the status of this effort. Where are we at?

Mr. KLOPP. Sure. So, in about 2010, we made the decision that this project was, we'll say, too big for the—our IT staff to execute. And so we did a competitive bid and outsourced the development of this system to Lockheed Martin and their partner MicroPact. They worked on this for several years. About the time I came in, it became clear to me that this was off track pretty badly. They had already spent about $300 million.

Mr. BLUM. I'm sorry to interrupt. Just in your professional estimation, how can it be off track when we're talking about that kind of money?

Mr. KLOPP. Yeah, you know, it's a great—it's a good question. I think how it gets off track is—is, in this particular case, I think that they just were off track from the beginning. I think the way they were trying to solve the problem fundamentally was broken. And, look, I mean, I'll be really clear. I think that for this to have gone as far as it did is a gigantic execution problem with our contractors and also a problem on oversight. We should never have let it go so far before we stopped it. I came in as CTO. Originally, I took a look at the architecture, suggested some——

Mr. BLUM. But if I could ask, what happened to the previous CEO—CIO?

Mr. KLOPP. The previous——

Mr. BLUM. I assume they were terminated——

Mr. KLOPP. No.

Mr. BLUM. —since it was off track?

Mr. KLOPP. No. The previous CIO was not terminated. I think that there was some shuffling around within our oversight group as people were sort of slapped for not overseeing this, right. You know, I mean, to be honest, there's a variety of places where oversight might have come from, and I think there was failure across the board there. So the previous CIO did not—was not fired as a result of this failure, but——

Mr. BLUM. Was he promoted?

Mr. KLOPP. No.

Mr. BLUM. Do you know if he was given—was he given a bonus?

Mr. KLOPP. No longer at the agency. Yeah, I don't know about that. That all happened before I came. So all I can say is, you know, with that regard, is I came in, saw it was off track, established some very objective engineering-level criteria to be able to demonstrate that the software that was being built was fundamentally broken. When in fact it was proven it was fundamentally broken, we shut the project down. We were still left with the problem that you identified, which is we had 54 disparate systems that ran on green screens that was just—it was just terrible. So, in October, we started a new project, which we called DCPS2, extremely modern, deployed in the cloud——

Mr. BLUM. October what year are we talking about?

Mr. KLOPP. Last year.

Mr. BLUM. Just last year.

Mr. KLOPP. Yeah, or a year ago in October. Yeah. So we've been at it for a little over a year.

Mr. BLUM. So this started in 2008, and in 2015, we started over after 7 years.

Mr. KLOPP. That's correct.

Mr. BLUM. And how many hundreds of millions were spent, would you estimate?

Mr. KLOPP. I believe that we spend $340 million up to the point that we shut it down.

Mr. BLUM. That's breathtaking.

Mr. KLOPP. Yeah, I don't disagree. Yep.

Mr. BLUM. I'm sorry. Continue. What is the status?

Mr. KLOPP. So the new system is now moving along at a, you know, proper pace. Currently, our run rate is about $25 million a year. So far less than these kinds of numbers that you heard be-

fore. We will deploy our first production release to the DDSes in December. So there will actually be cases running through this thing. So we're well past all of this, is it going to work; is it not going to work? That kind of stuff. And we believe that we're on the right path. And in fact, what we really believe is that—that we're—we're demonstrating, I think, in a really profound way that using the kind of modern software development techniques and cloud infrastructure that we would hope to be able to use over and over and over again if Chairman Hurd's bill gets through everybody, I think that this proves that we can modernize. And the cost of modernization is a fraction of these hundred million dollar projects. We will complete this project for significantly less than the money that was burnt last time.

Mr. BLUM. When's your estimation of when it will be complete?

Mr. KLOPP. You know, that's an interesting question. One of the odd things about agile software development, which is what we do these days, is that really we view these things not as projects anymore but as products. And like any product, we could continuously improve the product. As technology changes we would just try to incorporate those changes. And so the way we look at it is more of a question of, is the $25 million a year run rate that we spend on this, is it worth spending another $25 million next year for the enhancements that we can see in the backlog? So we view these—this thing as a product development, not as a project that will have an end.

Mr. BLUM. I'm from the private sector, and one thing that's very frustrating is, in Washington, D.C., there seems to be no penalty for failure. In fact, the answer usually to failure is: Let's spend more money. We're not spending enough of the taxpayer money.

And the money that we have wasted prior to you coming to the agency is absolutely stunning. It's breathtaking. This is what people are tired of. Is there a phase 1 document done on the design of the system that people signed off on, Lockheed—your contractor signs off on, people in government sign off on and say, "This is what we want built," and everyone agrees to it? Is there a document that's created before the first piece of code is programmed?

Mr. KLOPP. Yeah. So I believe the first time through, there was a detailed description of what needed to be built. I wouldn't call that an architecture document. The architecture and execution of building around those requirements was under the control of the contractors. So what we did is very clearly specified what we wanted them to build. And then there was an execution problem in actually getting that built.

Mr. BLUM. We need accountability. Either the contractors made a mistake and we shouldn't pay them, which would happen in the private sector, or the government officials who signed off in the agency made a mistake and they should be terminated. One or the other needs to be accountability, as I would think you would agree.

Mr. KLOPP. Yeah. So I would agree that there should be some accountability. The contract with Lockheed Martin and MicroPact was terminated. That was probably the best that we could do. I guess I will say, in the defense of the Federal workers that have to be responsible for this, is it's sort of tough if you—the program

basically punishes them for failure but doesn't really reward them much for success.

Mr. BLUM. And it's not the Federal workers that are the problem. It's the people at the very top typically or the contractors. One or the other.

But do you have a private sector background, by the way?

Mr. KLOPP. Yeah. I came just a couple years ago just to try to help out for a few years.

Mr. BLUM. Very good. Very good. Best of luck to you, and we'll be checking back in to see how the progress is. Thank you for your testimony.

I'm over my time, and I yield back, Mr. Chairman.

Mr. HURD. Before I go to Ms. Kelly, I'd like to ask a followup question on that, Mr. Klopp. Look, you're considered a political appointee, correct?

Mr. KLOPP. I am, yes.

Mr. HURD. So how do we prevent—you know, so $340 million was wasted. How do we prevent the DCPS from getting off the rails in a transition? Is that a fair question?

Mr. KLOPP. I think it is a fair question.

Mr. HURD. And, again, I don't know—either way, I don't know what the status is, you know, of the next administration and things like that. But if you're not going to be there to oversee it, how do we prevent this from—how do we prevent this from going off the rails?

Mr. KLOPP. I mean, I think it's a—I think it's a very fair question. I think one of the weirdest things for me as someone from the commercial world is the whole idea that the entire executive staff of not just the agency but the government is now about to transition out and transition in. There's no precedent for that in the commercial world.

What I will say is that, when I came in 2 years ago, I knew that I had a 2-year time limit. And so, from the very beginning, I started building an organization that was going to be capable of continuing on after I left. I've completely re-orged the system's organization. I've handpicked the people that report to me. I've handpicked the person that's running the DCPS project. And I'll actually tell you that I have no—I'm really—especially with regard to DCPS, I actually have no worries whatsoever about the continuing success of that project. The bigger idea of how to modernize the whole of SSA's IT organization I think is a much bigger challenge and has some cultural impacts. And I'm actually confident that we're going to do—that the people behind me are going to carry on and modernize that organization. But I'm leaving them with a much, much bigger job than the guy that's running DCPS.

Mr. HURD. So are there already plans in place to have a 2-week handover, 2-day handover, 2-hour handover? You know, what planning is ongoing to ensure a replacement is——

Mr. KLOPP. In the case of DCPS, I've been actually handing it over from the day I started, really. So that's why I said it—you know, you could have brought John Garrigues, the guy who is running that project from a technical perspective in and replaced me in this chair, and you would not have noticed any drop in quality. And I think that you're going to see this same thing when you hold

hearings, you know, 3 months, 6 months from now when I'm gone. I think you're going to see the people that I've handpicked behind are switched on. They understand what's going on. I mean, the Federal employees in the IT world, I think, are much more qualified than they normally get credit for.

Mr. HURD. Are you interested in staying?

Your comments are being recorded. We'll let you think about that and come back to you.

Ms. Kelly, you're now recognized for 5 minutes.

Ms. KELLY. I want to thank you, Mr. Klopp, for your thoughtfulness and not thinking, you know, who you work for but thinking about the American people and the industry and what will be a lasting effect instead of a short-term effect. So thank you for that.

In its fiscal year 2015 FISMA report to Congress, OMB reported a decline in FISMA compliance scores for our witnesses here today compared to their scores in fiscal year 2014. Does that mean that the state of cybersecurity's going in the wrong direction? No. The report caveats these results saying that a new scoring methodology has contributed to this decline in scores. In other words, you can't compare test results from fiscal year 2015 to fiscal year 2014 because the tests changed, and they got harder. So these results would not show the situation getting worse.

What they do show, Social Security, let's turn to you, the IG's audit made the significant conclusion about the choices you have made. The IG said, and I quote, "SSA focused its limited resources on higher risk weaknesses and therefore was unable to implement corrective action for all aspects of their prior year's deficiencies."

Now, Mr. Klopp, that sounds to me like the IG believes you made rational choices. You prioritized which problems you were going to address with the funds available to you. But you didn't have enough funding to correct all the vulnerabilities in the agency's IT systems. Do you agree with that?

Mr. KLOPP. I do agree with that. We have spent a lot of time trying to look and see what we need to do in order to be more effective at cyber specifically. And what we find is that—that, you know, the people are smart and capable. The way we prioritize taking things on are the way you would expect us to, picking off the high-value, you know, most significant vulnerabilities first. And the problem is that the—as we talked about in all of our—everybody's opening remarks, the threat level continues to raise and the funding that we have available to us in order to address that threat doesn't increase with the threat. In the case of Social Security, the funding available to IT is down 30 percent in the last 3 or 4 years. So we're trying to do more with less.

I think that, as I mentioned earlier, of the 59 findings from the IG audit, we were able to make progress in 58 of them. Frankly, the 59th one, we very explicitly elected to not make progress on. So it wasn't that we couldn't. But more funding would certainly help.

Ms. KELLY. With the lack of funding, how did you prioritize which problems to solve first? Did you consider the sensitivity of the PII that Social Security collects as one factor? Did you consider the severity of the weaknesses in your cybersecurity? How did you decide?

Mr. KLOPP. You know, I mean, I think that there's a couple of things we do. One is that we focus on sort of multilayered defense. And so when we saw vulnerabilities that had to do with the penetrating from the outside, those all become the highest priority things. When we find vulnerabilities on the inside that, if someone could get into, we focused on those high-priority items. You know, I'm not exactly sure—and I don't think the IG was very specific—I said in my oral testimony that we are—you know, the Department of Homeland Security does an audit of our outside penetration tests, and they've never found a critical vulnerability there and that, in the inside, when they look at those vulnerabilities, that we're consistently rated as being the second or third best as far as the least number of vulnerabilities. I mean, we have a very vibrant relationship with IG. And we actually think that there is a discrepancy between the way they evaluate us and the way Homeland Security evaluates us, probably a bigger discrepancy than in some other agencies. But it's okay. It just means that we—you know, everybody had that college professor that gave out tougher grades than other people, right? So we—we appreciate IG's tough remarks. But we probably would disagree that we prioritize wrong.

Ms. KELLY. Now, when it comes to funding, how much do you think you will need to plug up all of the holes?

Mr. KLOPP. I mean, that's a really interesting question. What I would say is that, you know, one of the problems we have is that all of the new modern products that would help us improve our cyber defenses, those products are being built for modern systems. They are being built for systems that will be deployed across large clusters of servers like in the cloud.

They are being built for systems that are deployed using modern service-oriented architectures and modern programming languages and stuff like that. And a lot of our systems predate all of those architectural things. And so for us to upgrade cyber to the level that you would like us to be at really requires the kind of modernization that we need from the bills that you guys are trying to push through. So we believe that we need a significant investment to fuel that modernization and get to the point where we could sustain modernization using sort of our—the base funding that we have now.

And we have asked for $300 million over 4 years in order to do that. And it's in the President's budget, that request.

Ms. KELLY. I yield back.

Mr. HURD. I'd like to now recognize the gentleman from the Golden State, Mr. Lieu for his 5 minutes of questions.

Mr. LIEU. Thank you, Mr. Chair.

After the devastating breaches at OPM, one of the things the administration did is they did this 100-day cybersecurity sprint where they wanted agencies to go to what's called two-factor authentication where, before you log on to your computer, to get in, you would need more than just a password. You would need a second form of authentication, either an ID card or something to that effect. Have you all done that?

Mr. ALBOUM. Yes, sir. At USDA, during the period of the Cyber Sprint and beyond, we have achieved—96 percent of our privileged users use PIV cards and 100 percent use either a PIV card or a

multifactor authentication tool, a token of some kind. And for our nonprivileged users, the rest of our workforce, we are at 92 percent for PIV cards presently.

Mr. LIEU. And your goal is to get to 100 percent for everyone at some point?

Mr. ALBOUM. That's the goal, but the reality is USDA has about 100,000 employees. There's turnover. It takes time from a point that someone comes on board to get them a PIV card. Our biggest opportunity is to dramatically decrease the time it takes for an individual to get a card once they come on board.

Mr. LIEU. Thank you.

What about NASA?

Ms. WYNN. At NASA, this is an area where we need to improve, and we understand that. And so where we are with our privileged users, during the Cyber Sprint, we made the 100-percent mark. For unprivileged users, this is where we have benefitted from having a permanent chief information security officer on board for a couple of months. And she has taken a hard look at how we measure it and who was considered in needing a PIV card. And so, for NASA, we will report one metric at the conclusion of fiscal year 2016. Our information is in process right now. But we are changing the universe of who needs to be covered by this requirement, so we are going to take a dip, and then we are going to go back up.

And we have—Charlie Bolden, the Administrator, has already met with the new Federal Chief Information Security Officer to give his assurance that NASA will get to 100 percent.

We believe it is going to take until the early part of 2018 to make that, but we will make significant progress in fiscal year 2017.

Mr. LIEU. Thank you.

What about SSA?

Mr. KLOPP. I get to show off a little bit. We are at 100 percent of our privileged users are using PIV cards. PIV cards are probably the most effective second factor because it's a physical thing you have to have in your hand. And, right now, we are at 98 percent of our unprivileged users. And, frankly, the reason we are only at 98 percent is because there's a small set of our unprivileged users who work in the 54 DDSes that was mentioned earlier. They are actually State employees, not Federal employees. And so it has just been slower for us to negotiate with the States and State unions and stuff like that in order to get that implemented.

But I believe that we are on track to get the last 2 percent of our unprivileged users onto PIV cards in December of this year.

Mr. LIEU. Thank you. Do you let some of your employees or all of them access their work email from their mobile devices?

Mr. KLOPP. No.

Mr. LIEU. Okay.

And how about NASA? Do you let any of your employees access their work emails from their mobile devices?

Ms. WYNN. Yes, we do. NASA has a very open environment designed for what—part of our mission is, is to share data openly with the public and academic and other institutions. We are taking a hard look and trying to thread the needle, so to speak, between that balance of being an open environment to exchange information, to advance technology and science and engineering, and bal-

ancing that against cybersecurity. Our new, as I mentioned before our new CISO is also taking a look at that too so that we find that delicate balance between being open and not putting our agency's mission at risk.

Mr. LIEU. I assume you have cybersecurity measures in place for your network systems, you know, desktop computers?

Ms. WYNN. Yes, we do.

Mr. LIEU. If someone is connecting from a mobile device, does your agency do anything to try to protect that mobile device?

Ms. WYNN. If it is a NASA-provided device, there are a lot of protections built into how we deploy it. If it's a personally owned device, we have protections for the network against that. But the device itself is not my responsibility. But if we should have a—if that device is creating a problem, we would act very swiftly on that point.

Mr. LIEU. So I see my time is up. I would like to just conclude. I think the mobile device of your NASA employees will be the weakest link in your defense system. And whether or not you view it as your responsibility, it can cause you grave problems if they are not protected.

Mr. HURD. Thank you, sir.

Mr. Klopp, you said at the beginning, the last of DHS technical vulnerability assessment, there were 16 progress recommendations or progress—16 recommendations that came from that? Is that correct?

Mr. KLOPP. That's correct.

Mr. HURD. And two were labeled—there were vulnerabilities or critical vulnerabilities?

Mr. KLOPP. Two were labeled as vulnerabilities. The rest were recommendations.

Mr. HURD. And you've addressed 8 of the 16 recommendations.

Mr. KLOPP. We have completely satisfied the 16 recommendations, including both of the critical vulnerabilities.

Mr. HURD. Both of the critical vulnerabilities. That was going to be my question. And then how are your own internal ongoing assessments working in conjunction with what DHS is doing?

Mr. KLOPP. The DHS assessments are what's called a red team assessment. And so, you know, we sort of let them in and let them snoop around. And then they make recommendations to us. It's actually not usual for them to identify specific vulnerabilities. It's more usual for them to provide these, sort of, general recommendations of where we need to go, pay some attention. So——

Mr. HURD. Are you just using automated tools?

Mr. KLOPP. Pardon me?

Mr. HURD. Are they just using automated tools?

Mr. KLOPP. Not just using automated tools. I think they actually bring some very highly qualified white hat hacker people in to go and try to work their way into the system.

Mr. HURD. And the times that they have come in, they haven't found vulnerabilities?

Mr. KLOPP. No, I wouldn't say that. What—for example, the last time they came in, we were able to stop them from penetrating through our sort of outer wall, and so we let them in. They, once in, found that they were having difficulty creating a beacon back

out. And so we let them create a beacon back out. And once they had—by the way, what the beacon out means is that, now that they are in, they can start navigating around because they can kind of control movement. And once we let them in and they found that they could move around, they actually found vulnerabilities in the system that we did not know existed and were able to identify those for us so that we could go get them fixed. That's exactly why we love these kinds of exercises, right?

Mr. HURD. No, it's a valuable resource and tool.

Mr. Alboum, so, in 2015, there was no major incidents at USDA. In 2015, no—there was no major—you saw no major incidents in 2015.

Mr. ALBOUM. That's correct.

Mr. HURD. You are monitoring 100 percent of the traffic at the external boundaries to determine if there is covert exfiltration of data. That's a good thing. I wish more people would be doing that. And you have deployed the EINSTEIN 3A capability fully, right?

Mr. ALBOUM. Yes, sir.

Mr. HURD. But the IG also still found that there was 26 outstanding recommendations that go back as far as 2009 and that 27 systems were operating with expired ATOs. And OMB scored y'all as—excuse me, that's the plural of "you" down in Texas—you got a 43 out of 100, the fourth worst score, and that's a decrease from fiscal year 2014. Are we looking at the right data?

Mr. ALBOUM. I think that's a good question. The, you know, the FISMA scores are based on the IG's interpretation of requirements, and I don't know that every IG interprets those requirements the same way. I think one of the things we can do as a community is agree on the metrics and how to score them and maintain the same metrics over a period of time so we can track improvement.

So you look at those scores, they demonstrate that USDA has opportunity to make further improvements. But the improvements that you'd note from 2014 are not the same improvements from 2015. And that makes it hard to track our progress. And being able to track progress and show positive movement I think is very important from a, not just a morale perspective, but a recognition of the programs we support. The money that's being spent on cybersecurity is making things better and not just going into some high IT black hole, which I know some people fear.

Mr. HURD. And that's fair, and I think that's what we try to do on this committee in a bipartisan way: give you the tools to be effective. Then we are going to hold you accountable, right? And we can always—the answer is always going to be, yes, we can have more money. But we have got to make sure that we are using the money that we have effectively and efficiently, because as we already talked about, we threw away $340 million. All right, let's not talk about some of the her interoperability at some of the other agencies. And so that's always kind of been our goal, and we are going to continue to do that.

And I appreciate y'all with your feedback today. It has given us food for thought and ideas on how to strengthen some legislation we are going to bring forward. And I appreciate you taking the time to appear before us today.

And if there's no further business, without objection, this subcommittee stands adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Statement of Congressman Gerald E. Connolly (VA-11)
Committee on Oversight and Government Reform, Subcommittee on Information Technology
Federal Cybersecurity After the OPM Data Breach: Have Agencies Learned their Lesson?
Rayburn 2154 10:00AM—November 16, 2016

Today's hearing is an important continuation of our efforts to ensure that the federal government dramatically strengthens its cybersecurity defenses, to best protect our constituents' sensitive personally identifiable information (PII) and defend our national security interests at home and abroad. Following the damaging breaches at the Office of Personnel Management (OPM), concentration on the implementation of the Federal Information Security Management Act (FISMA) and Federal Cybersecurity Enhancement Act of 2015 (FCEA) has never been more critical.

The devastating cyberattacks against our nation's federal and contract workforces represent the new normal of the 21st Century, where nation-states will, support attacks to gain access to sensitive information in foreign government computer networks, including intellectual property and classified national security information. The rapidly evolving nature of the cyber threat makes cybersecurity one of the most daunting challenges facing our nation.

However, securing federal information systems is not new problem. The security of federal cyber assets was placed on the U.S. Government Accountability Office's (GAO) High-Risk List in 1997. Suffice to say, meeting this threat has been difficult, confounding both Democratic and Republican Administrations and multiple Congresses. According to the U.S. Computer Emergency Readiness Team (U.S. CERT) data, over 8 years, the number of information security incidents reported by Federal agencies to U.S. CERT increased from 5,503 in Fiscal Year 2006 to 67,168 in Fiscal Year 2014, an increase of 1,121 percent.

Following the OPM data breaches, we sought to better understand precisely what happened to ensure that we have fully addressed and mitigated the threat. While it is important individuals and organizations that fell short of their obligations are held accountable, it is even more important that Congress and the Administration work together in a pragmatic and urgent fashion to ensure that the right statutory framework is in place to combat the advanced, persistent threat posed by our nation-state cyber adversaries. We must also ensure that in the aftermath of damaging breaches, those whose privacy has been threatened are protected from subsequent harm. OPM recently announced that, due to an expiring contract, identity protection services available to individuals affected in the massive data breaches will switch providers. I joined the Chairman and Ranking Member in sending a letter to OPM voicing concerns of potential

enrollee confusion throughout the transition and guaranteeing that no lapse in coverage will occur. Last Congress, I introduced the Fraud Reduction and Data Analytics Act of 2015 (HR 4180), which requires the Office of Management and Budget (OMB) to establish guidelines for federal agencies to establish financial and administrative controls to identify and assess fraud risks and design and implement control activities in order to prevent, detect, and respond to fraud.

I look forward to hearing about the progress being made implementing and deploying cutting edge security controls and monitoring abilities, and how legislation that requires the retirement of legacy systems such as the Federal Information Technology Acquisition and Reform Act (FITARA) and the Modernizing Government Technology Act (MGT or H.R. 6004) can help modernize federal IT systems.

The bottom line is that the race to harden America's cyber defenses is more aptly compared to a never-ending marathon than a quick sprint. Whether it is recruiting and retaining the next generation of cybersecurity professionals; addressing agency policies or statutory frameworks; authorizing information sharing, security standards, and cyber integration centers; or making good cyber hygiene as much of a social norm as washing one's hands after using the restroom; our nation must remained focused on strengthening federal cybersecurity.