

# **FINANCIAL SERVICES AND GENERAL GOVERNMENT APPROPRIATIONS FOR FISCAL YEAR 2016**

**TUESDAY, JUNE 23, 2015**

U.S. SENATE,  
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,  
*Washington, DC.*

The subcommittee met, pursuant to notice, at 10:33 a.m., in room SD-124, Dirksen Senate Office Building, Hon. John Boozman (chairman) presiding.

Present: Senators Boozman, Lankford, Coons, Mikulski, and Moran.

## **OFFICE OF PERSONNEL MANAGEMENT**

**STATEMENT OF KATHERINE L. ARCHULETA, DIRECTOR**

**ACCOMPANIED BY:**

**MICHAEL R. ESSER, ASSISTANT INSPECTOR GENERAL FOR AUDITS  
RICHARD A. SPIRES, CHIEF EXECUTIVE OFFICER, RESILIENT NETWORK SYSTEMS, INC.**

### **OPENING STATEMENT OF SENATOR JOHN BOOZMAN**

Senator BOOZMAN. The hearing will come to order.

The massive breach of the Office of Personnel Management (OPM) systems may be the most devastating cybersecurity attack in our Nation's history. Unfortunately, while the news reports about these incidents have been shocking, they should not be surprising. The OPM incident follows several across Government and is only the latest example of the Federal Government's inability to protect itself from cybersecurity threats.

Today's hearing before the Subcommittee on Financial Services and General Government is intended to elicit further information about the recent OPM data breaches. It is also a time to discuss the enormous challenges facing the Federal Government as it attempts to ensure this does not happen again.

The Government spends approximately \$82 billion a year on information technology. Given the cost of these projects and their impact on our economy and national security, members of the subcommittee have an ongoing commitment to conduct oversight. We must ensure that hard-earned tax dollars of millions of Americans are being spent wisely and effectively.

Just last year, the subcommittee held a hearing with OPM Director Archuleta, former Chief Information Officer (CIO) Steve VanRoekel, former General Services Administration (GSA) Admin-

istrator Dan Tangherlini, and the Director of Information Technology (IT) Management Issues at the Government Accountability Office (GAO) David Powner. Given the enormous resources and important security issues at stake, the subcommittee considered it imperative that the Office of Management and Budget (OMB) and Federal agencies appropriately managed these projects.

We're all well aware of examples of projects that ended in spectacular failure, as with the initial rollout of [healthcare.gov](http://healthcare.gov). While that kind of crisis makes news, we should also be troubled by the accounts that don't grab headlines, including initiatives with ongoing costs that grow each year after year without demonstrating effective results or sufficient security.

We must have safeguards in place to ensure that oversight of these projects are consistent, that problems are anticipated before they occur, and, most importantly, that someone is actually accountable and responsible. All too often, large complex IT projects drag on for years, outlasting the administration that initiated them and the employees responsible for managing them.

In the Financial Services and General Government bill alone, billions have been spent over the years on tax system modernization at the Internal Revenue Service (IRS), work that has been continuing for decades and is still incomplete. Even for projects now on track, past problems generate millions in additional costs and years of delay.

And as we have seen recently at IRS and once again with the OPM breach, both of which have compromised the personal data of millions of Americans, billions of Federal dollars spent are no guarantee of security. Across the Government, IT projects too frequently go over budget, fall behind schedule, and do not deliver value to taxpayers.

Responsibility for oversight is often fragmented throughout the agency owning the project, and OMB does not conduct appropriate review and management. Whether issues related to program requirements, performance, spending, or security, lots of people are involved, but often no clear lines of accountability are drawn.

What has happened at OPM is devastating. Millions of Americans and their families and friends have been affected. Giving those impacted limited free credit monitoring and identity theft insurance will not be enough to address the long-term consequences that we may see for years to come.

But also troubling is the knowledge that OPM is just the most recent example of the Government's systemic failure to protect itself. According to GAO, we should have serious concerns for the future. The number of information security incidents reported by Federal agencies has exploded in recent years.

Constant vigilance is required, and GAO has found that Government systems may not be prepared for the job. Nineteen of 24 major Federal agencies have reported deficiencies in information security controls. The Inspector General (IG) at 23 of those agencies cited information security as a major management challenge.

How many headlines of serious data breaches will it take to implement the steps necessary to protect ourselves? And at what point do some in Washington recognize that growing the bureaucracy without actually governing is a recipe for this type of disaster.

The Obama administration views the Federal Government as capable of tackling almost every problem that the Nation faces. Yet while attempting to grow the size and scope of the Federal Government at every turn, the administration fails to follow through on the tasks it is already responsible for. If you bounce from one bigger Government solution to another without carrying out your basic responsibilities, this is what happens.

It's easy to suggest more money is the solution. That seems to be the response the administration leans on every time there's a problem. But it is often the wrong choice, especially in situations like this where it appears that the problem is something much greater than a lack of resources.

The American people have lost faith in their institutions. The last thing they will do is trust Washington to solve a problem when it can't even protect the personal information of those it employs.

There needs to be a dramatic change in the status quo.

What I hope to hear from our witnesses today is not the same stale line that more money is needed, but an explanation as to why the Federal Government failed to do the basic job of protecting personal data of millions of employees with the vast resources it already has in hand, what it's doing right now to resolve this problem, and what is being done to ensure that we are prepared for the next attack.

I hope with your help we can learn from this incident and identify ways to improve and protect our security. I appreciate the interest of all my colleagues and our shared commitment to doing what we can to work together to try and address this so important issue. We cannot afford not to.

Senator Coons.

#### STATEMENT OF SENATOR CHRISTOPHER A. COONS

Senator COONS. Thank you, Chairman Boozman.

I'd like to welcome our witnesses, OPM Director Katherine Archuleta, Assistant OPM Inspector General Michael Esser, and former Department of Homeland Security (DHS) and the Internal Revenue Service (IRS) Chief Information Officer Richard Spires.

We are here today, as the chairman has laid out, to review information technology spending and data security at the Office of Personnel Management. As part of that review, we need to discuss recent cybersecurity attacks that have put Federal employee information and our national security at real risk.

We also need to address the late-breaking inspector general audit that expresses concerns about OPM's IT modernization project. But while we conduct this subcommittee oversight of OPM and its spending and response, I also urge us to put this in the context of larger cybersecurity challenges that face our Government and our society as a whole, and progress, or lack thereof, by Congress in strengthening our Nation's cyber defenses and in providing needed funding for Federal cybersecurity and IT initiatives.

Regarding the cyber incidents at OPM, one breach involved personnel data of roughly 4 million Federal employees stored on Interior Department networks. During the breach, investigators found another intrusion where information from background investigations was allegedly stolen.

I understand OPM only recently became aware of the security clearance theft and that the investigation is still underway. So while we may be limited in exactly what we can discuss in this context, I'm very hopeful we can have a productive and ongoing conversation.

The fact these security breaches happened is, frankly, terrible. They force us to grapple with the reality that in our interconnected world, we're more vulnerable than ever, and we need to do more to protect our public employees' vital personal information from foreign attackers.

After we've investigated why these cyber attacks were able to break through, we need to be willing to do what's necessary to ensure they don't happen again. These attacks don't just compromise the information of millions of Federal employees, but our Nation's security, as well.

It's further troubling the IG's office has found that OPM has not fully complied with the Federal Information Security Management Act, which mandates information security requirements for all Federal agencies. While OPM has made recent improvements, we need to remain vigilant.

Both Director Archuleta and the OPM CIO have only been on the job roughly a year and a half. And to their credit, they have made IT security a priority. But they need to clearly understand that the job is not done.

OPM has indicated to the subcommittee most of its IT security systems are aged and at the end of their useful life. For some, security patches are no longer provided by the original vendor. In fiscal year 2014, OPM began a 3-year IT system modernization and is seeking a third installment of \$21 million to complete that project this year. And we have to understand that without that funding, the investment of the two previous years can't be meaningfully completed.

I was alarmed by the IG's allegations about mismanagement of the modernization projects to date and hope that OPM's representatives will speak to these assertions directly here today.

Last, I just wanted to emphasize, I think we need to prevent another round of sequestration. OPM's fiscal year 2016 budget request includes a \$32 million increase over last year's enacted level, virtually all of which would address IT infrastructure improvements. Sequestration could critically threaten those investments and even the livelihoods of our employees.

While some of these cuts might be weathered in the short term, they can have serious long-term impacts. And I think we need to work together to ensure Federal agencies are prepared as best they can be to protect against cyber threats.

The Federal Government is at constant threat of cyber attacks. It successfully wards off millions of attempted attacks a year. And I think we need to work together to protect the Nation's economic and national security interests by coming together to deal with these vital cybersecurity issues.

Chairman Boozman, thank you for holding this hearing, and I'm eager to continue to work together as we consider the needs of our Federal agencies in combating cyber threats.

Senator BOOZMAN. Thank you, Senator.

Senator MIKULSKI. Mr. Chairman, may I just make a few comments and observations?

Senator BOOZMAN. You sure can. You can comment all you like.

Senator MIKULSKI. First of all, Mr. Chairman, I really want to thank you for your leadership in convening this hearing. I think America wants to know, certainly our Federal employees want to know, what happened and what is the impact on them, and what is the impact on the Nation.

I would strongly recommend to the chair that, after this hearing and then also the briefing we'll receive this afternoon, the chair and the ranking consider having a classified briefing, because as a member of both the Intel Committee and someone who has been involved on this, there are things that are best discussed that you need to know for your responsibilities in a setting. And Senator Cochran and I would be happy to cooperate with you in establishing that. You'll know more this afternoon.

The second point is, what has happened at OPM, and also what happened to the breaches at the Army, shows that this is a serious national issue. It affects not only OPM, but every agency, and also shows that national security and its impact is not limited to the Department of Defense (DOD).

Mr. Chairman, I also want to remind the committee or bring to their attention, we tried to deal with this in 2012. Under the leadership of Senators Lieberman and Collins, there was a bipartisan effort to have a cybersecurity bill that dealt with new authorities for key agencies to establish standards for critical infrastructure, create an info-sharing regime to protect both dot-gov and dot-com, and giving DHS authority to unite Federal resources across all levels of Government to have both the authorities to make sure they have the resources to know how to do the right job.

Exactly what you're saying, sir. Let's not just throw money at it. Let's get value and security for the dollar.

That was stopped because the Chamber of Commerce established a massive lobbying campaign, because they were worried that we would overregulate. Well, we are where we are.

So we need to do a lot of work. We had a bipartisan study group. They had people like Blunt, Coats, Collins, those of us on Intel and Approps. So maybe we need to resurrect that because it's OPM today, it'll be another agency tomorrow. We've got to make sure our cyber shields are up, we're fit for duty, and we're fit to protect our people.

So I just wanted to refresh everybody of that. And of course, my Federal employees need to know what happened, how do they protect themselves. And we need to know how to protect America.

So thank you, Mr. Chair.

Senator BOOZMAN. Thank you, Senator. And I think the suggestion of the classified briefing is an excellent one.

And also, this is, certainly, not a partisan issue. This is something that's been going on for a long, long time through successive administrations.

We have three witnesses appearing before us today: Katherine Archuleta, director of the Office of Personnel Management; Michael Esser, Assistant IG for Audits at OPM; and Richard Spires, CEO

of Resilient Network Systems and former Chief Information Officer at DHS and IRS.

Director Archuleta, I invite you to present your testimony.

SUMMARY STATEMENT OF KATHERINE L. ARCHULETA

Ms. ARCHULETA. Chairman Boozman, Ranking Member Coons, and members of the subcommittee, Government and nongovernment entities are under constant attack by evolving and advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused.

Unfortunately, these attacks will not stop. If anything, they will increase.

Although OPM has taken significant steps to meet our responsibility to secure personnel data, it is clear that OPM needs to accelerate these efforts, not only for those individuals personally, but also as a matter of national security.

My goal as director is to leverage cybersecurity best practices and protect the sensitive information entrusted to the agency, modernizing our IT infrastructure to better confront emerging threats, and to meet our mission and our customer service expectations.

OPM has undertaken an aggressive effort to update its cybersecurity. For fiscal year 2014 and 2015, we committed nearly \$67 million toward shoring up our IT infrastructure. In June of 2014, we began to completely redesign our current network while also protecting our legacy network.

These projects are ongoing, on schedule, and on budget. We implemented state-of-the-art practices, such as additional firewalls, two-factor authentication for remote access, and limited privilege access rights. We are also increasing the types of methods utilized to encrypt our data.

As a result of these efforts, in April 2015, an intrusion that predated the adoption of these security controls affecting OPM's IT systems and data was detected by our new cybersecurity tools. OPM immediately contacted DHS and the FBI. And together, we initiated an investigation to determine the scope and the impact of the intrusion.

In early May, the interagency incident response team shared with relevant agencies that the exposure of personnel records had occurred.

In early June, OPM informed Congress and the public that notification actions would be sent to affected individuals beginning on June 8 through June 19.

We are continuing to learn more about the systems that contributed to individuals' data potentially being compromised.

For example, we have now confirmed that any Federal employee from across all branches of Government whose organization submitted service history records to OPM may have been compromised, even if their full personnel file is not stored in OPM's system. These individuals were included in the previously identified population of approximately 4 million current and former Federal employees, and have been included in the notification.

Later in May, the interagency incident response team concluded that additional systems were likely compromised. This separate incident, which also predated the development of our new security

tools and capabilities, continues to be investigated by OPM and our interagency partners.

Based on this continuing investigation in early June, the interagency response team shared with relevant agencies that there was a high degree of confidence that OPM systems related to background investigations of current, former, and prospective Federal Government employees, and for those for whom a Federal background investigation was conducted, may have been compromised.

While we have not yet determined its scope and its impact, we are committed to notifying those individuals whose information may have been compromised as soon as practicable.

But for the fact that OPM implemented new, more stringent security tools in its environment, we would never have known that malicious activity had previously existed in the network.

In response to these incidents, OPM, working with our partners at DHS, has immediately implemented additional security measures to protect the sensitive information we manage. We continue to execute our aggressive plan to modernize OPM's platform and bolster security tools. We are on target to finish a completely new modern and secure datacenter environment by the end of fiscal year 2015, which will eventually replace our legacy network.

OPM's 2016 budget request included an additional \$21 million above 2015 funding levels to further support the modernization of our IT infrastructure, which is critical to protecting data from persistent adversaries that we face. This funding will help sustain the network security upgrades and maintenance initiated in fiscal years 2014 and 2015 to improve OPM's cyber posture, including advanced tools, such as database encryption and stronger firewalls and storage devices.

We discovered these intrusions because of our increased efforts in the last 18 months to improve cybersecurity at OPM, not despite them.

#### PREPARED STATEMENT

I am dedicated to ensuring that OPM does everything in its power to protect the Federal workforce and to ensure that our systems will have the best security posture the Government can provide.

Thank you and I appreciate the opportunity to testify today. I am happy to address any questions you may have.

[The statement follows:]

#### PREPARED STATEMENT OF KATHERINE L. ARCHULETA

##### A REVIEW OF IT SPENDING AND DATA SECURITY AT OPM

Chairman Boozman, Ranking Member Coons, and members of the subcommittee:

Government and non-government entities are under constant attack by evolving and advanced persistent threats and criminal actors. These adversaries are sophisticated, well-funded, and focused. Unfortunately, these attacks will not stop—if anything, they will increase. Although OPM has taken significant steps to meet our responsibility to secure the personal data of those we serve, it is clear that OPM needs to dramatically accelerate these efforts, not only for those individuals personally, but also as a matter of national security. When I was sworn in as the Director of the U.S. Office of Personnel Management (OPM) 18 months ago, I immediately became aware of security vulnerabilities in the agency's aging legacy systems and I made the modernization and security of our network and its systems one of my top priorities. My goal as Director of OPM, as laid out in OPM's February 2014 Stra-

tegic Information Technology (IT) Plan, has been to leverage cybersecurity best practices to protect the sensitive information entrusted to the agency, while modernizing our IT infrastructure to better confront emerging threats and meeting our mission and customer service expectations.

#### *Strengthening and Enhancing OPM's Data Security*

Over the last 18 months, OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. For fiscal years 2014 and 2015 we have committed nearly \$70 million towards shoring up our IT infrastructure. In June 2014, we began to completely redesign our current network, while also protecting our legacy network to the maximum extent possible in the interim. These projects are ongoing, on schedule, and on budget. The first phase of this project was to deploy the tools required to address critical vulnerabilities on the existing network. As part of this effort, in January 2015 we implemented state of the art practices, such as additional firewalls, two-factor authentication for remote access, and limited privileged access rights. Currently, we are also increasing the types of methods utilized to encrypt our data. These methods cover not only data at rest, but data in transit, and data displayed through masking or redaction.

As a result of these efforts to improve our security posture, in April 2015, an intrusion that predated the adoption of these security controls affecting OPM's IT systems and data was detected by our new cybersecurity tools. OPM immediately contacted the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) and, together with these partners, initiated an investigation and forensic analysis to determine the scope and impact of the intrusion. Shortly thereafter, OPM notified congressional leadership and select committees of this incident. In early May, the interagency incident response team shared with relevant agencies that the exposure of personnel records had occurred. That very same day, we worked to brief congressional leadership and select committees. In early June, OPM informed Congress and the public that notifications would be sent to affected individuals beginning on June 8 through June 19. We refer to this incident as the intrusion affecting personnel records.

As part of the ongoing investigation and analysis, we are continuing to learn more about the systems that contributed to individuals' data potentially being compromised. For example, we have now confirmed that any Federal employee from across all branches of Government whose organization submitted service history records to OPM may have been compromised—even if their full personnel file is not stored on OPM's system. These individuals were included in the previously identified population of approximately four million current and former Federal employees and are being appropriately notified.

During the course of the ongoing investigation, the interagency incident response team concluded—later in May—that additional systems were likely compromised, also at an earlier date. In late May, OPM and the interagency notified Congressional leadership and select committees of this separate intrusion. This separate incident—which also predated deployment of our new security tools and capabilities—continues to be investigated by OPM and our interagency partners. Based on this continuing investigation, in early June, the interagency response team shared with relevant agencies that there was a high degree of confidence that OPM systems related to background investigations of current, former, and prospective Federal Government employees, and those for whom a Federal background investigation was conducted, may have been compromised. We are currently working with our interagency partners to continue to offer classified briefings for members and staff on the status of this investigation. While we have not yet determined its scope and impact, we are committed to notifying those individuals whose information may have been compromised as soon as practicable. This separate incident is one that we refer to as the intrusion affecting background investigations.

But for the fact that OPM implemented new, more stringent security tools in its environment, we would have never known that malicious activity had previously existed on the network, and would not have been able to share that information for the protection of the rest of the Federal Government. In response to these incidents, OPM, working with our partners at DHS has immediately implemented additional security measures to protect the sensitive information it manages and to take steps toward building a simplified, modern, and flexible network infrastructure.

#### *Driving Continued Progress on IT Modernization*

We continue to execute on our aggressive plan to modernize OPM's platform and bolster security tools. We are on target to finish a completely new modern and secure data center environment by the end of fiscal year 2015 which will eventually

replace our legacy network. OPM's 2016 budget request included an additional \$21 million above 2015 funding levels to further support the modernization of our IT infrastructure, which is critical to protecting data from the persistent adversaries we face. This funding will help us sustain the network security upgrades and maintenance initiated in fiscal year 2014 and fiscal year 2015 to improve OPM's cyber posture, including advanced tools such as database encryption and stronger firewalls and storage devices.

#### *Conclusion*

As we are all aware, Government and non-government entities are under constant attack by evolving and advanced persistent threats and criminal actors. Again—we recognize that these attacks will increase. We are working with an interagency team to identify and rapidly implement protections that will decrease our risk; however, as we address critical immediate needs we also need to continue our work to address long-term strategic challenges that affect our ability to ensure the security of our networks in light of this persistent threat. As our OIG has noted, OPM has been challenged for several years in building and maintaining a strong management structure and the processes needed for a successful information technology security program. OPM agrees with this assessment which is why I prioritized development of the agency's Strategic IT Plan and have prioritized its implementation.

We discovered these intrusions because of our increased efforts in the last 18 months to improve cyber security at OPM, not despite them. I am dedicated to ensuring that OPM does everything in its power to protect the Federal workforce, and to ensure that our systems will have the best cyber security posture the Government can provide.

We thank you for your support of our ongoing efforts to strengthen our IT security and I appreciate the opportunity to testify today. I am happy to address any questions you may have.

Senator BOOZMAN. Mr. Esser.

#### SUMMARY STATEMENT OF MICHAEL R. ESSER

Mr. ESSER. Chairman Boozman, Ranking Member Coons, and members of the committee, good morning. My name is Michael Esser, and I am the Assistant Inspector General for Audits at the U.S. Office of Personnel Management. Thank you for inviting me to testify at today's hearing on the IT audit work performed by the OPM Office of the Inspector General.

Senator BOOZMAN. Can you put your microphone on? It's on? Just pull it closer then.

Mr. ESSER. Today I will be discussing OPM's long history of systemic failures to properly manage its IT infrastructure, which we believe may have ultimately led to the breaches we are discussing today, as well as issues related to OPM's current IT modernization project.

There are three primary areas of concern that we have identified through our Federal Information Security Management Act (FISMA) audits during the past several years: information security governance, security assessment and authorization, and technical security controls.

Information security governance is the management structure and processes that form the foundation of a successful security program. For many years, OPM operated in a decentralized manner with the agency's program officers managing their IT systems. This decentralized structure had a negative impact upon OPM's IT security posture, and all of our FISMA audits between 2007 and 2013 identified this as a serious concern.

By 2014, steps taken by OPM to centralize IT security responsibility with the CIO had resulted in many improvements. However,

it is apparent the OCIO is still negatively impacted by the many years of decentralization.

The second concern is security assessments and authorization. This process includes a comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate. We identified problems related to system authorizations in 2010 and 2011, but removed it as an audit concern in 2012. However, problems with OPM system authorizations have reappeared. In 2014, 21 OPM systems were due to receive a new authorization but 11 were not authorized by year-end.

In addition, the Office of the Chief Information Officer (OCIO) has recently put authorization efforts on hold until it completes the current modernization project. This action to extend authorizations is contrary to OMB guidance, which specifically states that an extended or interim authorization is not valid. It is also worth noting that OMB no longer requires systems to be authorized every 3 years, but that is assuming that agencies have implemented a mature continuous monitoring program.

Our FISMA auditing determined that OPM does not have a mature program. Therefore, we still expect OPM systems to have current authorizations.

The third concern relates to OPM's use of technical security controls. OPM has implemented a variety of controls and tools to make the agency's IT systems more secure. While this is obviously a positive step, we are concerned these tools are not being implemented properly and did not cover the entire technical infrastructure as we found that OPM does not have an accurate centralized inventory of all servers and databases.

Even if all the security tools were being used properly, OPM cannot fully defend its network without a comprehensive list of assets.

Also, there has been much discussion of the difficulty in securing OPM systems as they are old legacy systems. While this is true in many cases and many OPM systems are mainframe based, it is our understanding that some of the systems impacted by the breaches are, in fact, modern systems for which most of the technical improvements necessary to secure them could be accomplished.

In addition to the issues identified in our FISMA audits, I would also like to briefly address OPM's IT modernization project, which will overhaul its entire infrastructure and migrate all systems to a new data center environment. We recently issued a flash audit alert discussing this project and our concerns related to project management and the use of a sole source contract for the duration of the effort.

One area of significant concern that we identified is that OPM does not have a dedicated funding source for the entire project. Its estimate of \$93 million includes only the initial phases of the project, which covers tightening up the security controls and building a new shell environment. The \$93 million estimate does not include the cost of migrating approximately 50 major IT systems to this new shell environment. The cost of this work is likely to be substantial, and the lack of a dedicated funding source increases the risk that the project will fail to meet its objectives.

## PREPARED STATEMENT

In closing, it is clear that OPM has a great deal of work to do to strengthen its IT security posture. We fully support the concept of OPM's IT modernization project. However, especially for a task of this magnitude, it is imperative that OPM follow solid IT project management best practices to provide the project the best chance for success.

Thank you for your time. I'm happy to answer any questions you may have.

[The statement follows:]

## PREPARED STATEMENT OF MICHAEL R. ESSER

IT SPENDING AND DATA SECURITY AT OPM JUNE 23, 2015

Chairman Boozman, Ranking Member Coons, and members of the subcommittee:

Good morning. My name is Michael R. Esser. I am the Assistant Inspector General for Audits at the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing discussing the information technology (IT) spending and data security at OPM. Specifically, today I will be discussing the audits that the Office of the Inspector General (OIG) conducts in accordance with the Federal Information Security Management Act, commonly known as "FISMA." Although OPM has made progress in certain areas, some of the current problems and weaknesses were identified as far back as fiscal year 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today.

*OIG's FISMA Work*

FISMA requires that OIGs perform annual audits of their agencies' IT security programs and practices. These audits are conducted in accordance with guidance issued each year by the U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications. Today I will talk about three of the most significant concerns highlighted in our fiscal year 2014 FISMA report. However, it is important to note that our report contained a total of 29 recommendations covering a wide variety of IT security topics. Only 3 of these 29 recommendations have been closed to date, and 9 of the open recommendations are long-standing issues that were rolled-forward from prior year FISMA audits.

*1. Information Security Governance*

Information security governance is the management structure and processes that form the foundation of a successful information technology security program. Although the DHS FISMA reporting metrics do not directly address security governance, it is an overarching issue that impacts how the agency handles IT security and its ability to meet FISMA requirements, and therefore we have always addressed the matter in our annual FISMA audit reports.

This is an area where OPM has seen significant improvement. However, some of the past weaknesses still haunt the agency today.

In the fiscal year 2007 FISMA report, we identified a material weakness<sup>1</sup> related to the lack of IT security policies and procedures. In fiscal year 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT security policies. OPM's Office of the Chief Information Officer (OCIO) was responsible for the agency's overall technical infrastructure and provided boundary-level security controls for the systems residing on this infrastructure. However, each OPM program office had primary responsibility for managing security controls specific to its own IT systems. There was often confusion and disagreement as to which controls were the responsibility of the OCIO, and which were the responsibility of the program offices.

Further, the program office personnel responsible for IT security frequently had no IT security background and were performing this function in addition to another full-time role. For example, this meant that an employee whose job was processing retirement applications may have been given the additional responsibility of moni-

<sup>1</sup>An IT material weakness is a severe control deficiency that prohibits the organization from adequately protecting its data.

toring and managing the IT security needs of the system used to process those applications.

As a result of this decentralized governance structure, many security controls went unimplemented and/or remained untested, and OPM routinely failed a variety of FISMA metrics year after year. Therefore, we continued to identify this security governance issue as a material weakness in all subsequent FISMA audits through fiscal year 2013.

However, in fiscal year 2014, we changed the classification of this issue to a significant deficiency, which is less serious than a material weakness. This change was prompted by important improvements that were the result of changes instituted in recent years by OPM. Specifically, in fiscal year 2012, the OPM Director issued a memorandum mandating the centralization of IT security duties to a team of Information System Security Officers (ISSO) that report to the OCIO. In fiscal year 2014, the OPM Director approved a plan to further restructure the OCIO that included funding for additional ISSO positions. The OCIO also established a 24/7 security operations center responsible for monitoring IT security events for the entire agency; however, OPM has not yet implemented a mature continuous monitoring program.

This new governance structure has resulted in improvement in the consistency and quality of security practices for the various IT systems owned by the agency. Although we are optimistic that these improvements will continue, it is apparent that the OCIO continues to be negatively impacted by years of decentralized security governance, as the technical infrastructure remains fragmented and therefore inherently difficult to protect.

## *2. Security Assessment and Authorization*

A Security Assessment and Authorization (Authorization) is a comprehensive process under which the IT security controls of an information system are thoroughly assessed against applicable security standards. After the assessment is complete, a formal Authorization memorandum is signed indicating that the system is cleared to operate in the agency's technical environment.

The Office of Management and Budget (OMB) mandates that all major Federal information systems have a valid Authorization (that is, that they have all been subjected to this process) every 3 years unless a mature continuous monitoring system is in place (which OPM does not yet have). Although, as mentioned, IT security responsibility is being centralized under the OCIO, it is still the responsibility of OPM program offices to facilitate and pay for the Authorization process for the IT systems that they own.

OPM has a long history of issues related to system Authorizations. Our fiscal year 2010 FISMA audit report contained a material weakness related to incomplete, inconsistent, and poor quality Authorization packages. This issue improved over the next 2 years, and was removed as an audit concern in fiscal year 2012.

However, problems with OPM's system Authorizations have recently resurfaced. In fiscal year 2014, 21 OPM systems were due for Authorization, but 11 of those were not completed on time and were therefore operating without a valid Authorization.<sup>2</sup> This is a drastic increase from prior years, and represents a systemic issue of inadequate planning by OPM program offices to assess and authorize the information systems that they own.

Although the majority of our FISMA audit work is performed towards the end of the fiscal year, it already appears that there will be a greater number of systems this year operating without a valid Authorization. In April, the CIO issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through September 2016. Should this moratorium on Authorizations continue, the agency will have up to 23 systems that have not been subject to a thorough security controls assessment. The justification for this action was that OPM is in the process of modernizing its IT infrastructure and once this modernization is complete, all systems would have to receive new Authorizations anyway.

While we support the OCIO's effort to modernize its systems, this action to extend Authorizations is contrary to OMB guidance, which specifically states that an "extended" or "interim" Authorization is not valid. Consequently, these systems are still operating without a current Authorization, as they have not been subject to the complete security assessment process that the Authorization memorandum is intended to represent.

<sup>2</sup>The OIG is the co-owner of one of these IT systems, the Audit Reports and Receivables Tracking System. This system has been reclassified as a minor system on the OPM general support system (GSS), and cannot be Authorized until the OCIO Authorizes the GSS.

There are currently no consequences for failure to meet FISMA standards, or operate systems without Authorizations, at either the agency level or the program office level. The OIG simply reports our findings in our annual FISMA audit, which is delivered to OPM and then posted on our Web site. OMB receives the results of all FISMA audits, and produces an annual report to Congress. There are no directives or laws that provide for penalties for agencies that fail to meet FISMA requirements.

However, at the program office level, OPM has the authority to institute administrative sanctions. This could be an effective way to reduce non-compliance with FISMA requirements. We recommended that the performance standards of all OPM major system owners include a requirement related to FISMA compliance for the systems they own. Since OMB requires a valid Authorization for all Federal IT systems, we also recommended that the OPM Director consider shutting down systems that were in violation. None of the systems in violation were shut down.

Not only was a large volume (11 out of 47 systems) of OPM's IT systems operating without a valid Authorization, but several of these systems are among the most critical and sensitive applications owned by the agency.

Two of the OCIO systems without an Authorization are general support systems that host a variety of other major applications. Over 65 percent of all systems operated by OPM (not including contractor-operated systems) reside on one of these two support systems, and are therefore subject to any security risks that exist on the support systems.

Furthermore, two additional systems without Authorizations are owned by OPM's Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations. Any weaknesses in the IT systems supporting this program office could potentially have national security implications.

As I explained, maintaining active Authorizations for all IT systems is a critical element of a Federal information security program, and failure to thoroughly assess and address a system's security weaknesses increases the risk of a security breach. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

### *3. Technical Security Controls*

As previously stated, our fiscal year 2014 FISMA report contained a total of 29 audit recommendations, but two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication to IT systems using personal identity verification (PIV) credentials.

Configuration management refers to the policies, procedures, and technical controls used to ensure that IT systems are securely deployed.

OPM has implemented a variety of new controls and tools designed to strengthen the agency's technical infrastructure by ensuring that its network devices are configured securely. However, our fiscal year 2014 FISMA audit determined that all of these tools are not being utilized to their fullest capacity. For example, we were told in an interview with OPM personnel that OPM performs monthly vulnerability scans on all computer servers using its automated scanning tools. While we confirmed that OPM does indeed own these tools and that regular scan activity was occurring, our audit also determined that some of the scans were not working correctly because the tools did not have the proper credentials, and that some servers were not scanned at all.

OPM has also implemented a comprehensive security information and event management tool designed to automatically correlate potential security incidents by analyzing a variety of devices simultaneously. However, at the time of our fiscal year 2014 FISMA report, this tool was receiving data from only 80 percent of OPM's major IT systems.

During this audit we also determined that OPM does not maintain an accurate centralized inventory of all servers and databases that reside within the network. Even if the tools I just referenced were being used appropriately, OPM cannot fully defend its network without a comprehensive list of assets that need to be protected and monitored.

This issue ties back to the centralized governance issue I discussed earlier. Each OPM program office historically managed its own inventory of devices supporting their respective information systems. Even though the OCIO is now responsible for all of OPM's IT systems, it still has significant work ahead in identifying all of the assets and data that it is tasked with protecting.

With respect to PIV authentication, OMB required all Federal IT systems to be upgraded to use PIV for multi-factor authentication by the beginning of fiscal year

2012. In addition, OMB guidance also mandates that all new systems under development must be PIV-compliant prior to being made operational.

In fiscal year 2012, the OCIO began an initiative to require PIV authentication to access the agency's network. As of the end of fiscal year 2014, over 95 percent of OPM workstations required PIV authentication to access the OPM network. However, none of the agency's 47 major applications required PIV authentication. Full implementation of PIV authentication would go a long way in protecting an agency from security breaches, as an attacker would need to compromise more than a username and password to gain unauthorized access to a system. Consequently, we believe that PIV authentication for all systems should be a top priority for OPM.

Some of the other areas where we identified technical control weaknesses include:

- Operating system baseline configurations;
- Configuration change control;
- Tracking the status of known security vulnerabilities;
- Patch management;
- Termination of idle VPN connections, and;
- Continuous monitoring of security controls.

Finally, there has been much discussion of the problems with securing OPM's systems, as they are old, "legacy" systems. While this is true in many cases, and many of OPM's systems are mainframe-based, some systems that were impacted by the breaches are in fact more modern systems for which most of the technical improvements necessary to secure them could be accomplished.

#### *OPM's Modernization Project*

In April 2014, the agency began a full overhaul and modernization of its technical infrastructure, which will involve implementing additional IT security controls and then migrating the entire infrastructure to a completely new environment (referred to as the Shell). The OIG did not become aware of this project until nearly a year later, in March 2015, when we met with officials from the OPM's Office of the Chief Financial Officer and the OCIO to discuss questions related to the special \$21 million funding request for this project contained in the President's fiscal year 2016 budget.

On June 17, 2015, we issued a Flash Audit Alert detailing concerns related to project management as well as the use of a sole source contract for the entire project. One specific issue discussed in the Flash Audit Alert was funding for the project.

OPM informed us that the current estimate for this project was approximately \$93 million. However, after our auditors began their review, we learned that this cost estimate did not include the costs for migrating existing applications to the new Shell. That work is likely to be, by far, the most expensive part of the project. Migrating applications involves modifying all of the current systems—including all of the legacy systems that are frequently mentioned—so that they can operate in the new Shell environment. In 2009, OPM undertook a similar effort with its financial system application, and it cost \$30 million and took 2 years. There are approximately 50 major systems that have to be migrated to the Shell, and many smaller ones.

Moreover, I am very concerned with the lack of an adequate funding plan for this project. Although there is a \$21 million special request in the President's fiscal year 2016 budget, and DHS has committed \$5 million to the project, there is no comprehensive plan to fund the remaining costs of the project. Instead, we were told, in essence, that the OCFO would find the remaining funds somewhere, meaning a very heavy burden will fall upon program offices that are already stretched thin. The annual appropriations of program offices are meant to fund their core mission responsibilities, not subsidize a major agency-wide IT infrastructure project.

This last issue has also become significantly problematic for our own office. Because we were unaware that OPM had undertaken this immense project, we were unable to include the related costs in our fiscal year 2016 budget request. The project will impose three types of costs upon us: (1) increased oversight costs, (2) the payment of the special assessment since we are a user of OPM IT services, and (3) the costs of modifying OIG-owned systems that reside on OPM's network so that they are compatible with the new IT environment.

#### *Conclusion*

As discussed above, OPM has a history of struggling to comply with FISMA requirements. Although some areas have improved, such as the centralization of IT security responsibility within the OCIO, other problems persist. Until OPM's security weaknesses are resolved, OPM systems will continue to be an inviting target for attackers.

If OPM's new modernization project is implemented appropriately, we believe that it will significantly improve OPM's IT operations, including its IT security posture. However, there are several issues, including significant budgetary concerns, which must be addressed. If they are not, we fear that there is a high risk this project will fail to meet its stated objectives.

Thank you for your time and I am happy to answer any questions you may have.

Senator BOOZMAN. Thank you, Mr. Esser.

Mr. Spires.

#### SUMMARY STATEMENT OF RICHARD A. SPIRES

Mr. SPIRES. Good morning, Chairman Boozman, Ranking Member Coons, and members of the subcommittee.

I'm honored to testify today. And since I served as the Chief Information Officer of the Internal Revenue Service (IRS) and later the Department of Homeland Security (DHS), I hope my in-the-trenches experience is of value regarding recommendations I will make on how the Federal Government can more effectively safeguard data and improve its cybersecurity posture.

Most Federal Government agencies find themselves susceptible to data breaches and compromises of core mission IT systems because of three primary root causes.

First, lack of IT management best practices. The very best cybersecurity defense is the result of managing your IT infrastructure and software applications well. But beginning in the 1990s and up to the present, the Federal Government has not properly managed IT, having failed to effectively adapt with the changes in IT technology and the evolving cybersecurity threat.

As examples of these failures, when I served in Government, we would all too routinely discover IT systems outside of the IT organization's purview that have been deployed without the proper IT security testing and accreditation. The highly distributed approach to IT management across Government, and I would point out that Mr. Esser in his testimony already referred to decentralization within the OPM environment itself, has led to the deployment of thousands of data centers. Federal agencies struggle with managing and maintaining this dispersed infrastructure and disparate systems.

The resulting complexity of vastly different systems and underlying IT infrastructures makes it virtually impossible to properly secure such an environment.

Second, lack of IT security best practices. While well intentioned and appropriate for the time, the 2002 Federal Information Security Management Act (FISMA) skewed the approach for Government IT information security. The law forced the Chief Information Security Officers (CISOs) to look at the controls for individual systems, when in reality viewing systems in isolation hid the impact of larger enterprise security posture.

Further, until very recently, systems would be certified and accredited based on a 3-year cycle, which is a significant issue when looking at the rapid evolution of technology in the cyber threat environments.

Third, a slow and cumbersome acquisition process. When I was at DHS, I was a proponent of continuous diagnostics and mitigation, or the continuous diagnostics and mitigation (CDM) program. But it is dismaying to see how long it took, 2-plus years, just to

implement phase one. That does not include the additional competitive process for an agency to obtain capabilities. Sophisticated adversaries will exploit any and all vulnerabilities. The Government is even more vulnerable when it takes months, not years, to be able to deploy new IT security capabilities.

My recommendations to address these root causes: First, effectively implement the Federal IT Acquisition Reform Act, or FITARA. This law is meant to address the systemic problems in managing IT effectively, and the main intent of the law is to empower the agency CIO to address these issues.

So far, I am pleased with the approach of the OMB and the new CIO Tony Scott are taking to support FITARA's rollout. Congress can support these efforts by demanding aggressive implementation of FITARA by agencies, development of measures for assessing FITARA's impact, and transparency in reporting ongoing progress.

Effective implementation of FITARA is the Government's best hope to address decades of IT mismanagement.

Second, drive adoption of IT security best practices. There has been positive movement with the updated FISMA law and the move to continuous monitoring. Yet I recommend the Government rethink how it is measuring success, with focus along three lines.

There is a continuing need to pursue cybersecurity tools to prevent intrusion, but even more importantly, detect them quickly when intrusions do occur. Yet the Government needs to assume that sophisticated adversaries will still gain access.

The root of all trust is verified identity, and the Government needs to step back and rethink how it is rapidly implementing ubiquitous use of multi-factor identity authentication, along with the behavioral detection systems to identify insider threats or compromise credentials.

Finally, the Government needs to target additional protection of an agency's most sensitive information. Through focused effort and the use of available data protection technologies, the Government can attain high assurance that only the trusted parties have access to an agency's most sensitive information. This would go a long way toward thwarting additional major and damaging data breaches.

Certainly, the data breaches at OPM are terrible for the Government and for those millions of us who may be negatively impacted in the future. However, this episode and the need to implement FITARA and the new FISMA law can be the impetus for much-needed and sustained change.

#### PREPARED STATEMENT

It is critical to make enough progress during the next 18 months to ensure that leadership commitment to needed changes in IT management and security are sustained into the next Congress and administration.

Thank you for the opportunity to testify today.  
[The statement follows:]

#### PREPARED STATEMENT OF RICHARD A. SPIRES

Good morning Chairman Boozman, Ranking Member Coons, and members of the subcommittee. I am honored to testify today in regards to the recent Office of Per-

sonnel Management (OPM) data breaches, while addressing issues and making recommendations regarding approaches on how the Federal Government can more effectively safeguard data and improve its cybersecurity posture.

Serving as the CIO of a major department (DHS) as well as the CIO for a large bureau (IRS) in the Department of Treasury, I had ample opportunity to understand the dynamics inherent in Federal Government information technology (IT), including how Government agencies generally dealt with their IT security vulnerabilities. While at the IRS and DHS, I worked closely with the Chief Information Security Officers (CISOs) at both organizations to implement approaches that would address these security vulnerabilities. I also worked across the Federal Government on these issues, serving for a period as the Vice Chair of the Federal CIO Council and also as the Co-Chair of the Committee for National Security Systems. Given the gravity of this issue, I hope that my testimony is of value to Congress and the administration in helping to address systemic weaknesses in how the Federal Government protects data and its IT systems from compromise.

Please note that I never worked at OPM and while I will allude to some of the alleged details of the recent OPM data breaches, my testimony describes broader systemic issues that must be addressed if we are to better protect our Government's data and IT systems. In fact, I would urge Congress and the administration to avoid a tactical approach that addresses narrow technical fixes based on these latest breaches—the weaknesses that led to these types of breaches are deeply rooted and require sweeping changes in our approach to IT and cybersecurity management and practices. Further, the weaknesses in the Federal Government's IT security posture are almost always based on IT practices that have been in place over many years. I served in the Bush and Obama administrations and saw the same systemic problems in both. This should not be viewed as a political issue, but a call to action to fix a set of issues that can not only have a beneficial impact on securing data and systems, but improve IT management and delivery of systems as well.

My testimony will first focus on identifying the root causes that have led to a situation allowing massive data breaches of sensitive data and personally identifiable information (PII) to occur in Government. I will then provide a set of recommendations to address these root causes that can, based on my experience, be implemented over a 2-to-3 year timeframe. As I describe below however, there is a window of opportunity to drive these changes that Congress and the administration cannot afford to miss.

#### ROOT CAUSES OF IT SECURITY AND DATA PROTECTION VULNERABILITIES

The situation in which most Federal Government agencies find themselves susceptible to data breaches and compromises of core mission IT systems, are the result of three primary root causes, which include:

##### *1. Lack of IT Management Best Practices*

The very best cybersecurity defense is the result of managing your IT infrastructure and software applications well. During the decades of the 1970s and 1980s, agencies could build and deploy IT systems with little regard to security issues. This was not necessarily a management failure since there were very few security issues to be concerned with prior to the broad use of the Internet and the rise of the ubiquitous data networks. However, beginning in the 1990s and up to the present, the Federal Government has not properly managed its IT. The Government has failed to effectively adapt with the changes in IT and the evolving cybersecurity threat.

As example of these failures, when I served at IRS and then at DHS, we would all-too-routinely discover IT systems outside of the IT organizations purview that had been developed and deployed without the proper IT security testing and accreditation. This highly distributed approach to IT management has led to the deployment of thousands of data centers across the Federal Government. Federal agencies today struggle with managing and maintaining this dispersed infrastructure and disparate systems. In far too many instances, hardware and software assets are not systematically tracked, software is not routinely updated and patched, and critical hardware and software has reached end-of-life and, in some cases, is no longer even supported by the vendors. And while I am big proponent of cloud technology, I am concerned that many agencies are not necessarily using cloud capabilities to streamline and simplify their infrastructure, but rather creating new IT "stovepipe" infrastructures. This complexity of maintaining a sea of vastly different systems in an ocean of differing underlying IT infrastructures makes it increasingly impossible to properly secure such a complex IT environment.

Worse, when the Government did realize it had these issues and attempted to fix them, entrenched interests made it exceptionally difficult to effect the necessary changes. For instance, a number of laws have been passed that attempted to ad-

dress IT management practices, most notably the Clinger-Cohen Act of 1996, which mandated a strong agency CIO that could begin to rationalize IT within an agency. Yet Clinger-Cohen is viewed as failed legislation in the Federal IT community since in reality, none of the agency CIOs have the authority granted by Clinger-Cohen. Components, Bureaus, and program offices have generally resisted efforts to bring more oversight and discipline to IT management and operations under the theory that it impedes mission and business progress for agencies. Unfortunately, we are paying a huge economic cost for those decisions resulting in inefficiency, duplication and unsecure IT systems and infrastructure. And what is now worse; we will likely pay a greater cost in the exposure of PII of millions of current and former Government employees, and potentially a cost to our national security.

## *2. Lack of IT Security Best Practices*

While well intentioned and appropriate for its time, the Federal Information Security Management Act (FISMA) skewed the approach for Government IT information security. Originally passed in 2002, it set a course for how IT security effectiveness has been measured in Government. While there are some good components of the law, the unintended consequence is that it forced CISOs to look at the controls for individual systems when in reality, IT systems across the Government were already becoming more interconnected and viewing systems in isolation hid the impact on the larger enterprise security posture. Further, based on OMB guidance, FISMA was implemented during a period when the cyber-threat was still emerging and the evolution of technology hadn't yet recognized the necessity of a security development lifecycle. In fact, until very recently, systems would be certified and accredited based on a 3-year cycle, which, while perhaps manageable, is comical when looking at the rapid evolution of technology and the cyber-threat environment. And furthermore, the law required the generation of paper-based reports, which diverted time, resources and personnel from effective security efforts. At both IRS and then DHS, I was consistently reluctant to put my confidence in the yearly FISMA report since it did not reflect the reality of the true security posture of our overall IT environment. That can only be done by proper use of tools that continuously monitor the IT environment and are able to react and mitigate threats in near-real time.

## *3. Slow and Cumbersome Acquisition Process*

The problem is exacerbated for Government when funds are available to invest in IT security, yet it is ponderously slow and difficult to buy commercial solutions to help address vulnerabilities. When I was at DHS, I was a proponent of the continuous diagnostics and mitigation (CDM) program, but it was dismaying to see how long it took (2 plus years) just to implement Phase 1, and then for agencies to go through an additional competitive process within the CDM program itself to obtain capabilities. I am all for fair competition, but with sophisticated adversaries that will exploit any and all vulnerabilities, the Government is even more vulnerable when it takes many months (if not years) to be able to deploy new IT security capabilities.

### RECOMMENDATIONS FOR ADDRESSING IT SECURITY AND DATA PROTECTION VULNERABILITIES

Clearly the Federal Government's overall IT security posture is poor, yet there is some momentum building that can result in fundamental changes that greatly improve that posture over a couple of years. While it is disappointing to have such large and damaging data breaches occur at OPM, I hope that the Congress and the administration use this opportunity as a call to action for needed IT and IT procurement reform. Below are four recommendations to address the root causes for the IT security and data protection vulnerabilities outlined above.

#### *1. Effectively Implement the Federal IT Acquisition Reform Act (FITARA)*

In December 2014 Congress passed and the President signed FITARA, which was included in the 2015 National Defense Authority Act (NDAA). FITARA is meant to address the systemic problems in managing IT effectively in an agency and while there are a number of provisions, the main intent of the bill is to empower the agency CIO to address these problems. Foremost of these problems include duplication of IT infrastructure and systems, lack of the use of best practices in IT acquisition, and the implementation of proper procedures to ensure IT security is properly addressed throughout an agency's IT organization and infrastructure.

To ensure that FITARA does not suffer the same fate as Clinger-Cohen, a successful roll-out within agencies is critical. I am very pleased to see the approach OMB and the new Federal CIO, Tony Scott, are taking to support this roll-out. OMB just issued its final guidance to agencies for implementation of FITARA. In developing

this guidance, OMB sought significant outside input, including guidance from former Government CIOs, CFO, CAOs, CHCOs, and COOs and importantly, OMB asked for public comment on this draft guidance, which will improve content, understanding, and buy-in over the longer term.

I recently testified at a hearing on FITARA and its role in improving IT acquisitions to the subcommittees for Information Technology and Government Operations of the House Committee on Oversight and Government Reform.<sup>1</sup> I am not going to repeat much of that testimony, but I want to highlight the following:

“In terms of accountability, it has to start with the Administration and rests with OMB and the agencies. In particular, OMB must help ensure that the agency CIOs have the capability to perform their job and have the support from agency leadership to give them the chance to drive the required change to effectively implement FITARA. Further, the agency leadership must be supportive of the agency CIO, having the individual's back, particularly in agencies that are operating in a federated environment (this is particularly an issue in the cabinet-level departments). Congress . . . can support these efforts by demanding aggressive implementation of FITARA by agencies, development of measures for assessing FITARA's impact, and transparency in reporting of ongoing progress, while also highlighting obstacles in agencies to be overcome.”

There is much confusion regarding IT security and the best way to protect data and systems. There is no single product or service that offers complete protection, and in my experience, without IT management best practices implemented across an agency, many of the security tools are simply ineffective. IT management best practices are foundational to success, and effective implementation of FITARA is the Government's best hope to address decades of mismanagement.

## 2. Drive Adoption of IT Security Best Practices

To the Government's credit, there has been a fairly aggressive shift in thinking from the traditional FISMA reporting approach to continuous monitoring of IT systems and the overall IT environment. I was also pleased to see that Congress passed much needed reform in the FISMA Modernization Act of 2014 last December, and I hope Congress will closely work with the executive branch to ensure that implementation delivers enhanced security.

That being said, when I look at the current Cross-Agency Priority (CAP) cybersecurity goals,<sup>2</sup> I feel the Government is still behind current IT security best practices. For example, if you look at the overall objectives, the CAP goals will typically consider objectives of less than 100 percent as success, such as 95 percent for automated asset management or 75 percent for strong authentication. Higher numbers are certainly better than lower ones in these metrics, but we are dealing with adversaries that are advanced and persistent, that will almost certainly find the holes and exploit them—it is simply a matter of time. Likewise the Einstein system can aid agencies in detecting threats, and the promise of Einstein 3A is the proactive blocking of malicious traffic. However, Einstein is only helpful if the traffic is actually going through the system—in many agencies today, there are Internet connections that are not monitored by Einstein and I posit that this is another example of poor IT management. The Government has invested hundreds of millions of dollars in the Einstein program yet agencies continue to posture and delay implementation. In effect, these approaches have led the Federal Government to establish a virtual “Maginot Line” as its key IT security strategy.

Based on the current situation and what I see evolving in the cybersecurity industry, I recommend a rethinking of how we are measuring success, with focus along three lines:

—There is without a doubt a continuing need to pursue cybersecurity tools to prevent intrusions, but perhaps even more importantly, detect them quickly when intrusions do occur. The Einstein program identifies and protects against known “signatures” or characteristics of malicious activities, thereby preventing those intrusions. However, more advanced protective capabilities are required to prevent intrusions that the Government is not yet aware of, thereby further reducing the Government's attack surface. With enhanced automated protection, network defenders can then focus on detecting and remediating only the most sophisticated and potentially dangerous attacks—rather than trying to decide

<sup>1</sup> Richard Spires written testimony for that hearing is available at <https://oversight.house.gov/wp-content/uploads/2015/06/Spires-Statement-6-10-FITARA.pdf>.

<sup>2</sup> A description of the CAP cybersecurity goals and the status can be found at <http://www.performance.gov/node/3401/view?view=public#overview>.

which of the seemingly endless alerts to pursue today. The cybersecurity industry has made great strides in these areas in the last few years, and Government should be using the most advanced tools for prevention and detection that leverage threat intelligence from users all over the world.

- Even with the most advanced prevention tools, the Government needs to assume that sophisticated adversaries will still gain access. So alternative approaches are needed, and in particular, ones that relies on creating more trust in online interactions. The root of all trust is verified identity. I must know that it is who I believe it to be, and in the online world, multi-factor authentication methods are key to doing that. There are a plethora of newly available technologies to enable multi-factor authentication for both internal (Government) as well as external users. And some of these solutions can integrate with antiquated systems. The Government needs to step back and rethink how it very rapidly implements ubiquitous use of multi-factor identity authentication. Even though the root of trust is identity, there is more to the trust equation. In the “physical” world, I trust another because I have high confidence they will act in a manner that I expect. Some of the most damaging data breaches have come from individuals that were properly authenticated and authorized to use systems and access data. Their behavior, however, was not in keeping with what was expected. This is commonly called the insider-threat problem. There are new technologies and capabilities today that can bring in other context, such as an audit log or behavioral analysis systems to assess someone’s trustworthiness on a regular basis. These additional factors, beyond those used to assess authenticity, are key to fully establishing and monitoring trust.
- Finally, the Government needs to target additional protection of an agency’s most sensitive information, whether it be data sets or documents. Tools and products exist that enable agencies to protect information, independent of the likely insecure environment in which they operate. Agencies should focus on their most valuable information. I do recognize that there are limitations given some of the antiquated systems in which such information resides, but by focusing efforts on the most sensitive information, the Government could ensure, within two to 3 years, that only trusted parties have access to an agency’s most sensitive information. This would go a long way toward thwarting additional major and damaging data breaches.

### *3. Attract, Train, and Retain Talented Cybersecurity Professionals*

Even the best cybersecurity tools in the world require talented people who know how to use them. The shortage of cybersecurity professionals across the country continues to be significant problem. This is particularly an acute problem for the Federal Government. While the mission is very attractive to many cyber professionals, the hiring process and compensation models are not competitive with what individuals can make in the private sector. Even with direct hiring authority, the Government is not getting the talent it needs. The Government needs more investment in training for current staff and the flexibility to hire that is competitive with the private sector. I do commend Congress for incorporating new flexibility for DHS to hire and pay cyber professionals into S.1691 also passed last December. Congress should monitor how DHS uses this authority, and consider expanding the authorities to other departments and agencies to help address the Government’s cybersecurity personnel shortage.

### *4. Develop a Streamlined IT Cybersecurity Acquisition Process*

It is difficult to implement state-of-the-art IT cyber security solutions if you have no way to rapidly evaluate them before purchasing. The CDM and Einstein programs could potentially serve as governmentwide vehicles for this process, but it has taken significant time to put them in place and I recommend an approach that enables individual agencies to rapidly bring in solutions and try them in a test-bed environment. After thorough testing and based on what works best, agencies should be able to roll security solutions into production. This approach would ideally encompass traditional cybersecurity vendors, but also new vendors that have little to no Government experience—they are an incredible source of technical innovation. The Government is simply not getting the best solutions through the existing acquisition process. I recommend that Office of Federal Procurement Policy (OFPP) work with the General Services Administration (GSA) and DHS to put a more streamlined CDM in place—one that would enable rapid addition of new capabilities as they become available in the commercial market.

## CONCLUSION

Certainly the data breaches at OPM are terrible for the Government and for those millions of us that may be negatively impacted in the future. Viewed through the right lens however, this episode can be the impetus for much needed and sustained change. And given the need to implement FITARA, the current administration has a golden opportunity to set the correct foundation for success moving forward. This should not be viewed as a political issue but rather requires sustained leadership focus and commitment, and I am pleased to see such leadership currently coming from both Congress and the administration. It is critical to make enough progress during the next 18 months to ensure that leadership commitment to FITARA, FISMA Modernization and to other needed changes in IT security are sustained into the next Congress and administration.

Thank you for the opportunity to testify today.

Senator BOOZMAN. Thank you, Mr. Spires, for your testimony.

At this time, we had planned on proceeding with our questioning. Each Senator will have 7 minutes. I hope we have time to accommodate two rounds of questioning.

We have a vote called right now. It is only one vote. So what we would like to do is suspend, allow members to vote, and then come back and start immediately with the question period.

With that, we will adjourn.

[Recess.]

Senator BOOZMAN. The committee will come to order. Again, I apologize for the delay. The only thing we have to do around here is vote, and so there is just no way of knowing. You schedule these things and, certainly, that trumps everything, which it should.

Director Archuleta, according to news reports about the second OPM breach pertaining to OPM's security clearance system, hackers had access to sensitive data for a year. These systems contain extensive personal and family financial information for current, former, and perspective Federal employees and contractors.

Will a notification be provided to individuals whose information was potentially compromised in the latest breach?

## NOTIFICATION

Ms. ARCHULETA. Yes, sir. We are working on determining the scope of that breach, even as we speak. And as we determine that, at the same time, we are developing a notification process to reach those individuals.

We are taking into account what we have learned from the first notification and looking at the wide range of options we would have in that notification process.

Senator BOOZMAN. Will notifications be provided to family members and other individuals whose information was contained in the security clearance system solely due to their relationship with the security applicant?

Ms. ARCHULETA. Sir, I can say that we are taking into consideration all of the individuals that were affected by this breach. As that notification plan is developed, I would welcome the opportunity to come up and detail it for you.

Senator BOOZMAN. How did you decide that 18 months of credit monitoring and identity theft insurance is sufficient protection for affected Federal employees?

Ms. ARCHULETA. This is an industry best practice. We are, again, in the second notification really examining that to see what the range of options may be.

Senator BOOZMAN. Will OPM offer the same protection to individuals whose information was stored on security clearance databases, or does this heightened level of compromised information warrant additional protections?

Ms. ARCHULETA. Again, sir, this is what we are looking at with our partners across Government to make sure that we examine the wide range of options that we need to consider.

Senator BOOZMAN. What additional steps do you plan to take to protect the victims, given the long-term effects these breaches pose?

Ms. ARCHULETA. We are looking at steps we can take to protect their data including the notification process. I am as upset as they are about what has happened and what these perpetrators have done with our data. So we are examining not only the notifications that we must do, but also the protections and the remedies we must put in place.

Senator BOOZMAN. Those are important questions. Those are the kinds of things we are getting from our Federal workers. I know you will have a lot more other questions related to that. But it is so important that we try to get information to those that have been affected.

Ms. ARCHULETA. I understand.

Senator BOOZMAN. Mr. Spires, the administration has ordered a 30-day sprint to perform vulnerability testing and to patch security holes. Is 30 days sufficient time to correct more than a decade of negligence of outdated systems and failed attempts at modernization?

Mr. SPIRES. I'm sure you would not be surprised for me to say no, it is not sufficient time to fix the systems and the situation we find ourselves in.

I think it is a good thing, though, to put in place a process by which planning should take place, so that we can start to get our arms around what should be done agency by agency to put us in a much better posture.

Senator BOOZMAN. As we get into these things, Mr. Spires and Mr. Esser, do you expect us to find significant problems as far as breaches with the other agencies?

Mr. SPIRES. First, I should say you will find significant problems with them not following IT security best practices, including FISMA, and not that that alone would necessarily indicate breaches. But given the situation we find ourselves in across most Federal agencies, I would expect you to find significant breaches, yes.

Senator BOOZMAN. Mr. Esser.

Mr. ESSER. I would concur with Mr. Spires.

We have been seeing breach after breach this year, health insurance companies, background investigations, contractors, and Government entities, so it would not surprise me to see more.

Senator BOOZMAN. Mr. Spires, again, looking at the scope of the problem, how long do you feel like it will take the Government to actually do things we need to do to protect ourselves from these outside threats?

Mr. SPIRES. Well, let me say, I think we should take an ordered approach to this problem. So in my mind, what agencies should

first be doing is identifying the sensitive datasets they have and putting those in some type of bucketed priority order, and coming up with plans to protect those sensitive data sets.

The reason I say it that way is to think that we can go into these large agencies that have, as I said, decades of mismanagement and essentially decentralized IT and fix that quickly I think is just naive. So this notion of doing it by protecting sensitive data sets, then there is data technology today and encryption and the like, to do that at the data set or document level. And then also, you have to worry about the identity problem. It does no good if you have encrypted the data, but then the credentials of someone that can get to the data have been compromised. So you also need to work on the identity problem.

That is where things like multi-factor authentication models come in, which, by the way, there are many new technologies that make this much faster and easier to roll out than it was 4 or 5 years ago.

Also, this notion that says even if someone has been authenticated and authorized, that doesn't necessarily mean their behavior is correct, right? The insider threat problem, we have to watch that.

So this notion of starting to bring in behavioral detection systems or ways in which we can monitor the behavior of, particularly, privileged users. Those that have root access to the systems and data are the ones that, frankly, we need to monitor.

Senator BOOZMAN. Very good.

Director Archuleta, we have heard numerous accounts of frustration with CSIdentity Corporation (CSID), including long wait times, repeated Web site crashes, and inaccurate information reported to victims. What steps are you taking to oversee the services provided by the contractor?

#### CONTRACTOR OVERSIGHT

Ms. ARCHULETA. CSID has tremendous experience in these types of notifications. They served Sony, as you know, with their large breach. We believe they have the capability and capacity to handle this.

Senator BOOZMAN. But when you call in now, the wait times are very, very long. I don't know that they have experienced anything of this magnitude.

Ms. ARCHULETA. Thank you, sir. I am as angry as you are about that. I want to be sure they are doing everything they can to reduce wait times. That is why I have instructed my CIO and her team to work with that contractor to improve daily the services they are giving to our employees.

An employee should not have to experience that. That is why we are demanding from our contractor that they improve their services.

I do believe, sir, because of the conflation of two incidences, that we have had an unusual high number of phone calls. But that is not an excuse. Our contractor should be able to perform to that number, and we are demanding that it do so.

Senator BOOZMAN. Thank you.

Senator COONS. Thank you, Chairman Boozman.

Ms. Archuleta, if I might, if OPM had completed its planned IT upgrades, would this breach have been prevented? Would these consequences have been prevented?

And if OPM had been in full compliance with FISMA, would any of the breaches in 2014 or 2015 still have occurred?

#### IT UPGRADES

Ms. ARCHULETA. My CIO has advised me that even if there had been 100 percent FISMA compliance, there is no guarantee that systems won't get breached. That is why an IT strategic plan and the implementation of an IT plan is so important. Risk management is the answer to what we need to do. We need to be able to detect and mitigate. That is what our plan is designed to do, as we move from a legacy system to the new shell system.

Yes, I believe we need to act very rapidly to move from this decades-old system to a new system. We need to make sure that we are tracking, documenting, and justifying all we do. But we also need to be sure we are acting as quickly as we can to protect the records that have been entrusted to us.

Senator COONS. Ms. Archuleta, of all of the Federal employees who have been affected, as the co-chair of the Senate Law Enforcement Caucus, I am particularly concerned about Federal law enforcement officers and their families, because they have credible reasons to be concerned. The criminals they previously apprehended or investigated might have motivation to seek out their homes or their families.

What are you doing specifically to promptly respond to their concerns or inquiries? Not to suggest they're the only folks with real concerns, but in some ways they are one of the subsets of Federal employees who I think have very real, very legitimate and pressing concerns.

Ms. ARCHULETA. On the top line, what I can assure you, Senator, is that we are working across Government to analyze the scope of this breach. We will be able to discuss more with you in the classified session.

But I can tell you that we are working very closely with our law enforcement partners.

Senator COONS. I am eager to follow up with you on that and to get some reassurance about the swiftness with which gravely concerned Federal employees of all backgrounds are able to get updates and more information about their path forward.

Your fiscal year 2016 budget request was submitted before the discovery of the most recent incident and before we had any sense of the scope. Are there additional tools or enhancements that you need in order to deal with the critical issues that are now well and widely known? And how might you seek an amendment to the budget request?

#### IT FUNDING

Ms. ARCHULETA. Thank you, Senator, for that question.

We are analyzing right now with OMB and my CFO to determine what the request might look like. I hope to be able to get back to you by the end of the week.

Senator COONS. Thank you.

Last question for you, if I might: If you had actually encrypted Federal employees' Social Security numbers or their personally identifying information, would that have prevented the disclosure of their personally identifiable information to hackers once they compromised the system?

#### ENCRYPTION

Ms. ARCHULETA. This is a question that has been asked of my colleagues who are experts in cybersecurity. They have informed me that in this particular case, the encryption would not have prevented the breach.

Encryption is an important tool, and that is why we continue to build the encryption methods within our system. But in this particular case, it would not have prevented it.

Senator COONS. My question was not whether it would have prevented the breach. It was whether it would have prevented the accessibility and use of personally identifying information once the system was breached.

Ms. ARCHULETA. No. It would not have in this case.

Senator COONS. In response to the question about FISMA compliance and if IT upgrades had been completed and encryption, Mr. Spires, Mr. Esser, any difference of opinion or any insights you might offer for us about FISMA and whether FISMA compliance would have produced a different outcome here?

Mr. SPIRES. As I stated in my verbal testimony, sir, the issue with FISMA, the old FISMA 2002 law, was that it was really around a set of technical controls that would be checked every 3 years. Given the environment we live in, that is just not even close to being appropriate.

We are moving toward a continuous diagnostics model, which is the correct model, where you are monitoring all of your systems and monitoring your complete environment, looking for intrusions, looking for improper behavior.

But I would even echo the point that even that is not enough in today's environment. You need to bring in the data protection, like encryption capabilities, and you need to upgrade the capabilities to better understand who is actually accessing your system.

Those are all critical necessities in order to protect data today.

Senator COONS. Would it be reasonable for us to have expected that OPM could achieve data security given the resources they currently have available to them?

Mr. SPIRES. I am not sure I'm in a good position to answer that question. I will go back to my point of a focused effort on protecting sensitive data with the right encryption and the right access control capabilities. If you put the focus there, I think most Federal agencies would have the funds, have the resources to be able to accomplish that.

Senator COONS. We have seen significant data breaches for Home Depot, JPMorgan, Target, Sony, Neiman Marcus, just to name a few. Many of them have invested in cutting-edge cybersecurity and systems.

Is the private sector having any more success in mitigating cyber breaches than the public sector is?

Mr. SPIRES. I don't know if I would make a sweeping comment on that. I think it depends a lot on the actual company, and it varies greatly. I would make another point here.

I think one of the big differences between the Government and the private sector is that the private sector has the ability to very rapidly acquire the newest capabilities that are being offered by the cybersecurity, if you will, product companies or industry.

One of the things I would like to see is the Government agencies being able to bring in, in a test-bed environment, be able to pilot new capabilities as they come to market. That would really help Government agencies to adopt the newest capabilities.

Senator COONS. You referenced in your previous testimony the Federal IT Acquisition Reform Act (FITARA) and your concerns about slow and cumbersome procurement, and I look forward to exploring that further with you in the next round of questions.

Thank you, Mr. Chairman.

Senator BOOZMAN. Senator Lankford.

Senator LANKFORD. Thank you all for being here. We have a lot to cover to be able to help not only resolve things for the future, but also be able to unpack fully what has happened in the past.

Mr. Esser, there are several comments that you made on it. What is the most pressing issue that you have discovered in the flash report you have done, based on the vulnerabilities that still exist and what needs to be finished?

I am not asking you to expose publicly vulnerabilities that still exist, but on the list, how many things still need to be addressed and need to be addressed immediately?

Mr. ESSER. Senator, I think one of the most important things that needs to be addressed is the two-factor authentication to access systems. This has been a longstanding problem at OPM. They have made improvements. They have implemented this to affect workstation access. But the actual systems that are being used by employees need to be implemented also and require two-factor authentication.

Senator LANKFORD. I saw from your report and, quite frankly, the Chief Information Officer had also listed the same thing in 2012.

Let me just read this real quickly. The initiative to require personal identity credential authentication to access the agency network, as of the end of 2014, 95 percent of OPM workstations required personal identity verification access for the network. However, none of the agency's 47 major applications require personal identity verification authentication.

Is that still correct?

Mr. ESSER. To the best of our knowledge, it still is.

Senator LANKFORD. Ms. Archuleta, tell me about that and just the process of transition.

#### IG RECOMMENDATIONS

Ms. ARCHULETA. Yes, two points there. The multifactor authentication for remote users, we are 100 percent at that point now. With regard to all other users, we are working very rapidly to increase that. I have asked my CIO to increase that effort. I'm sorry

I don't have the percentages in my mind right now, but I would be glad to get back to you where we stand as of this date.

But I do know we are working rapidly to do that.

Senator LANKFORD. A 95 percent figure you think is pretty close as far as the workstations, 100 percent for those working remote, 95 percent of workstations, but it is still these 47 major applications that are still exposed, I guess?

Ms. ARCHULETA. I would like to get back to you, Senator, on that, to give you the full details on that.

Senator LANKFORD. Okay. Then there is a question on the issue of security assessment and authorization.

Obviously, that is a requirement from OMB. This ongoing issue of these 47 different groups that are here, it says 11 were not completed or time or were operating without a valid authorization.

What can you tell me about that?

Ms. ARCHULETA. I can tell you that all but one of those systems has been authorized or extended. They are operating with authorization, and we are working on the final one that was with the contractor.

Senator LANKFORD. There is a systemic problem there, obviously, of trying to find out why they weren't already through the authorization, to make sure that authorization is done on time and on schedule. Has that issue been fixed?

I know rapidly people stepped in and said, okay, let's try to fix this, where the authorizations haven't been done. What about the process for future, to make sure those continue to be done on time?

Ms. ARCHULETA. I would like to have my CIO get that information so I could give it back to you, sir.

Senator LANKFORD. I'll be glad to have that. Give me a time-frame when I can get that back.

Ms. ARCHULETA. By the end of the week, sir.

Senator LANKFORD. That would be great.

There is also an outstanding letter that I sent to your office June 10. I am the chairman of the Committee on Homeland Security Governmental Affairs that has the Federal workforce in it, as you and I have discussed in the past.

On June 10, I sent a letter that has yet to be acknowledged from your staff that they have received that letter, much less get an answer to it. There were some very basic questions that are still unanswered on it, none of them that would require a classified setting. But there are some basic responsive answers.

I have letters already on the record from the Federal Aviation Administration (FAA), for instance, and a tremendous number of employees that live in my district that have asked just some very basic questions. The folks from GE have asked some very basic questions. They have yet to get a response even to say it has been acknowledged. They just want to know some timing.

I know the letters have gone out nationwide. But people want to know there is actually somebody working on some of these other issues because there will be many for a while.

Ms. ARCHULETA. Senator, I apologize to you if you have not received that response. I know that I have asked my staff to respond to that, and I know that it is forthcoming. But I will make sure you have that letter today.

Senator LANKFORD. Great. Thank you.

Let's talk a little bit about cost issues dealing with the appropriations side.

Do we have a ballpark cost to OPM yet, the letter that has gone out to contact everyone to let them know, hey, possibly your information has been breached?

There are really two cost factors sitting out here that our committee has to consider. One is the cost of distributing that letter out to all those individuals. The second one is the cost for the credit report, credit screening and protection that is happening, that has been extended.

Do you have a cost estimate for those two?

#### CONTRACT COST

Ms. ARCHULETA. I have a general cost as we take a look at the take-up rate on credit monitoring, that will adjust it, but it is approximately anywhere from \$19 million to \$21 million.

Senator LANKFORD. Okay, so \$19 million to \$21 million.

And then what is the estimated cost on just the letter going out?

Ms. ARCHULETA. That is the total cost, sir, between emails and letters, so I do not have the breakdown. I would be glad to get that for you.

Senator LANKFORD. Are you aware that some agencies, actually the Web site you link people to to get more information, some agencies have actually blocked that internally. So those individuals when they try to go are blocked for fear there may be phishing scams that are going on.

So have you started working with other agencies on that?

Ms. ARCHULETA. Yes, we worked closely with departments and agencies because of some security protocols they might have. So we worked closely with them and their CIOs and other top officials.

Senator LANKFORD. Finally, this issue of the inventory of servers and databases and different workstations that are out there, the central control issue is important, obviously, for keeping up security and technology upgrades, and making sure software is continually upgraded, and everyone has a consistent security presence there.

When there is a server there, it creates tremendous vulnerabilities. They just have to find one of those.

How is that going with unifying that structure, because that is not a legacy issue. That is more just an inventory issue.

Ms. ARCHULETA. I respect the inspector general's opinion on this, but my CIO has told me that we have indeed have an inventory of system and data, and I would welcome the opportunity to discuss this with you and with him further.

Senator LANKFORD. Great. We will look forward to getting that report and getting a chance to find out more about that.

Ms. ARCHULETA. Thank you, Senator.

Senator LANKFORD. That is one of those significant vulnerabilities.

Ms. ARCHULETA. Thank you, sir.

Senator MORAN. Mr. Chairman, thank you and Senator Coons for conducting this hearing.

Welcome to our three witnesses.

Ms. Archuleta, I am going to begin with you. I just have a series of questions that I hope are relatively short responses. I will work my way through them as quickly as I can.

What is the current estimate of the total number of files or employees breached?

#### OPM DATA

Ms. ARCHULETA. In the employee personnel files, we estimate that to be a little over 4 million.

Senator MORAN. At least according to press reports, those numbers may grow. What else may occur? What may you discover?

Ms. ARCHULETA. It is an ongoing investigation. We will continue that investigation with our partners. At this point, we know it is a little over 4 million.

Senator MORAN. Are those words interchangeable, 4 million employees and 4 million files? Does that mean the same thing?

Ms. ARCHULETA. That is approximately 4 million people who have been affected by it.

Senator MORAN. What is the total possible for the number of employees affected? You say we estimate it today to be 4 million and it may grow. What is the maximum number of files that could have been breached?

Ms. ARCHULETA. I want to separate incident one and incident two. So incident one is the one I am describing, the employee personnel files. We have estimated that to be a little over 4 million, as I have described.

Senator MORAN. But what is the total number of employees that could be affected by that?

Ms. ARCHULETA. That is the number.

Senator MORAN. That is the number?

Ms. ARCHULETA. That is the number.

Senator MORAN. All right.

Ms. ARCHULETA. So as we look at the second incident, we have not determined the scope of that. I don't have a number for you on that.

Senator MORAN. How many files do you have management over?

Ms. ARCHULETA. As you know, a Federal background investigation file may have a number of different names and Personally Identifiable Information (PII) within it. That is why I cannot give you a specific number on that one.

We are working, as I said, to get that number. I will bring it to you as soon as I have it.

Senator MORAN. Let me ask this one more time to make sure that you and I are on the same page.

Ms. ARCHULETA. Okay, I apologize if I am not fully understanding.

Senator MORAN. No, it may be inarticulation on my part.

You have a certain number of files within your agency subject to this kind of breach. What is the total number of files that potentially could be breached?

Ms. ARCHULETA. That is what we are investigating right now, sir.

Senator MORAN. Let me ask it this way, how many files are there at OPM?

Ms. ARCHULETA. Well, there are millions of files. We are a data center, so there are millions of files. The forms SF-86 or the background investigations contain numerous names. That is why I want to be careful to make sure the number I do give to you I'm confident about.

Senator MORAN. All right.

You indicated you have taken significant steps. I wrote that down as part of your testimony. "We have taken significant steps." Yet the OIG says that only three of 29 recommendations have been closed. Let me look at his testimony. "Only three of these 29 recommendations have been closed to date. Nine of these open recommendations are longstanding issues that were rolled forward from prior year FISMA audits."

How do you reconcile, "We have taken significant steps," and yet the OIG report says there are longstanding problems and only three of 29 have been addressed?

#### IG RECOMMENDATIONS

Ms. ARCHULETA. We work very closely with our IG. As I said before, we work with him to make sure that we have complete and open transparency with him. We meet on a regular basis. He continues to assist us in identifying the areas of improvement. And the issues he has brought to us, we are working through.

The 2014 audit that he performed for us and provided to us, we are working through the steps that he has outlined for us. I know we are not in agreement with all of them, but we do believe that the conversation and the transparency that we have between us will be helpful for resolving all of them.

Senator MORAN. Mr. Esser, do you agree with Ms. Archuleta that the agency has taken significant steps to correct its problems?

Mr. ESSER. Yes, I do. I think that they have made great strides over the years to improve some of the issues we have reported.

For example, the decentralization issue, which went back to 2007, in this past year's FISMA audit, we decreased the severity of that finding from a material weakness to a significant deficiency.

In addition, there are a number of other areas where they put in tools and made strides to improve security.

With that said, there are a number of longstanding issues in our FISMA reports that are open and that we hope to see movement on.

Senator MORAN. Mr. Spires, let me give you an opportunity. If you were still in the former capacity at this agency instead of the IRS or Homeland Security, let me first start with a broader question. Based upon your understanding of the facts involved here and your best judgment, was the breach or breaches that have occurred at OPM, were they predictable, based upon what we knew, looking at, for example, the OIG report? If you saw those reports, is this an outcome that could be expected?

Mr. SPIRES. I think it is an outcome that could be expected, sir.

Senator MORAN. Do you have a sense based upon either Ms. Archuleta's testimony or your independent knowledge and what you have heard of Mr. Esser and their reports, would you say that the OPM officials have taken significant steps to solve their problems?

Mr. SPIRES. It does sound like they are doing a number of the things correctly. I think the centralization of IT is a very good step. They're talking about a modernization program that would upgrade their IT infrastructure.

That being said, I go back to my earlier point that if I had walked in there as a CIO—and again, I am speculating a bit—and I saw the kinds of lack of protections on very sensitive data, the first thing that we would have been working on is how to protect that data, not even talking about necessarily the systems. How is it we get better protections and then control access to that data better?

I think that is probably where the focus needs to shift here, based on what I am hearing.

Senator MORAN. Meaning that out to be a priority, the first effort.

Mr. SPIRES. Yes.

Senator MORAN. Ms. Archuleta, does anyone at OPM take personal responsibility for these breaches, or is this just considered a problem with the system?

Is this a problem with individuals not performing their duties? Or it is just that this is the system we inherited, we're working on it, and no one, in particular, is responsible for the outcome?

#### STATE OF FEDERAL IT

Ms. ARCHULETA. I think Mr. Esser and Mr. Spires said it very correctly. This is decades of lack of investment in the systems that we inherited when I came in. From the very beginning of my tenure, I have been focused on this.

We are working to install not only the architectural strategies, but also to install the detection systems and be able to remediate.

But as both of my colleagues have mentioned, we have legacy systems that are very old. Oftentimes, we have to test to be sure we can even add those protection systems into the legacy system.

If there is anyone to blame, it is the perpetrators. Their concentrated, very well-funded, focused, aggressive efforts to come into our systems not just at OPM, but as both of my colleagues have said, across the whole enterprise, is one we are concerned about and one we are working with our colleagues.

We are going to take every step we possibly can at OPM to continue to protect. That is why we are trying to move out of the legacy system.

Senator MORAN. To date, you don't consider anyone at OPM, any of your staff or employees or people responsible for IT and security to be personally responsible? It is a problem with the system that has been inherited?

Ms. ARCHULETA. This is an enterprise-wide problem, and cybersecurity is the responsibility of all of us who head organizations. That is why, with the Tony Scott's assistance and with his efforts, we are going to address this on an enterprise-wide basis as well as OPM.

Senator MORAN. So no one is personally responsible?

Ms. ARCHULETA. I don't believe anyone is personally responsible. I believe that we are working as hard as we can to protect the data

of our employees, because that is the most important thing we can do.

I take it very seriously. I'm angry, as you are, that this has happened to OPM. I'm doing everything I can to move as quickly as I can to protect the systems.

Senator MORAN. Thank you very much.

Ms. ARCHULETA. Thank you, sir.

Senator BOOZMAN. Mr. Esser, Ms. Archuleta mentioned that the problem is with the legacy systems, which I think we would all understand. However, isn't it true that several of the breaches were not to legacy systems, and with the right tools in place they would not have been breached?

Mr. ESSER. Yes, sir. Based on our audit work.

Senator BOOZMAN. So the idea that this is all legacy systems is really not the case.

Mr. ESSER. Well, there are many legacy systems at OPM. I don't want to give the wrong impression. I mean, that is a fact. But based on the work that we have done in our audits and ongoing work that we are doing, it is our understanding that a few of the systems that were breached are not legacy systems. They are modern systems that current tools could be implemented on.

Senator BOOZMAN. Okay, very good. I think that is really important.

Concerns are being raised about the contract secured to provide credit-monitoring services to the victims of the first breach. We don't know the scope of the second breach and what services will be provided for additional victims.

Mr. Esser, in your flash audit, you raised concerns about OPM's sole-sourced contract to manage OPM's infrastructure improvement project related to subsequent phases of the project. Do you have additional work planned to oversee OPM's contracting and procurement practices?

Mr. ESSER. It is, certainly, something that we are monitoring and following the reports and gathering information. We haven't planned any audits of that at this time, but it is something we may do.

Senator BOOZMAN. Very good.

Mr. Spires, you describe a number of root causes that have led to the current issues the Government faces in IT security, and you have offered a number of recommendations.

Can you just tell us again a couple of key recommendations that would make a difference over the next year or two?

Mr. SPIRES. Yes, I would really like to reemphasize FITARA. I thank Congress for passing it for the good of the Nation. We need to figure how to manage our IT more effectively.

I would say that is the single root cause that has led to these kind of situations we find ourselves in with these data breaches. It's not that I'm just one to say we need to have all the power reside with the CIO. But what we need are CIOs that have the authority to really bring best practices and not allow systems or practices to continue that jeopardize the security of our data and our systems.

That has been the problem for decades. We still have real cultural problems. I mean, I am out of Government now for 2 years,

but based on many discussions I have had with brethren that are still CIOs and still in Government, the cultural issues loom large here.

We need to take this incredibly seriously. And I would urge you as a subcommittee to provide your own oversight of the implementation of FITARA.

Senator BOOZMAN. Do we need additional legislation?

Mr. SPIRES. I am not convinced. I think we do need the general cyber legislation about how we better share information between the Government and the private sector. I think that is something that Congress should continue to work on.

I think we have, between the FITARA act and between the updated FISMA act, I think we have enough tools on the legislative side. I think it is now a leadership and management set of issues within the administration, with the proper oversight of Congress.

Senator BOOZMAN. Very good.

Mr. Esser, along the same line, what would you identify as the most significant weaknesses or the underlying causes? What do you see as the priority we need to do in the next 2 or 3 years?

Mr. ESSER. Specific to OPM, I think the project they are undertaking to modernize the IT systems is the right way to go. That definitely needs to be done. We fully support that project.

We do have some concerns, as expressed in our flash audit alert, regarding some of the project management issues related to it, and the sole-source contracting. But in general, we think it is definitely the right path to follow.

Senator BOOZMAN. So how will you all be involved? Mr. Spires talked about oversight. Certainly, that is something we will do in this committee. How will you be involved in that process?

Mr. ESSER. We are continuing our oversight of the modernization project. The flash audit alert was issued this week. It was just an interim report, so to speak. We are going to continue our audit work throughout the length of this project.

Senator BOOZMAN. Mr. Spires, the administration's cyber goals are an effort to drive significant and rapid improvement and changes, yet that is not working. Do you recommend any changes to the goals?

Mr. SPIRES. Yes, I would first comment that I think having goals is, certainly, appropriate, but let's take one example, this notion we all talked about, this need for multifactor authentication, to be able to much better protect the credentials of those who use these systems that are legitimate. Yet when you look at the cyber goal and you look at the use of, for instance, the Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) card and trying to get the 75 percent usage within the civilian Federal agency as the goal, let's go back to the adversaries. They only need one way in, right? And 75 percent just doesn't cut it in this world anymore.

So we need to rethink, I think, the objectives there. Go back to the prioritization of protecting data, doing the multifactor authentication. Those should be the highest goals.

That does not mean we shouldn't be working to continue to bring in the right kind of capabilities to better protect our systems. We

need to do that as well. But I think it is time to rethink those goals and to reset them along those sets of priorities.

Senator BOOZMAN. Mr. Esser, you mentioned that one of your findings was that OPM didn't exactly know what inventory they have. Is that being corrected? Or do we still not know the number of units, servers, hardware components, etc.?

Mr. ESSER. Based on our latest work, that is still our understanding. Director Archuleta commented a little while ago that they do have a complete inventory of systems, so we would be more than happy to work with them and look at that and do our audit work related to that.

Senator BOOZMAN. But if that is a case, that has just recently happened?

Mr. ESSER. Yes, sir.

Senator BOOZMAN. Okay, thank you very much.

Senator COONS. Mr. Chairman, I will defer to the vice chair of the full committee.

Senator BOOZMAN. Senator Mikulski.

Senator MIKULSKI. Thank you very much.

Mr. SPIRES, could you tell me, has Kaspersky been penetrated? I understand even top-notch security firms themselves sometimes have a cyber shield that can be penetrated.

Mr. SPIRES. I do not have any more information than what I read in the news, Senator, but I read that as well.

Senator MIKULSKI. Which indicates that this is an international problem.

Mr. SPIRES. It certainly is.

Senator MIKULSKI. It really shows that, despite best efforts of highly skilled professionals—that is not to excuse where we are—but your advice to us is to get with it, and get with it pretty quick.

Mr. SPIRES. You summed it up very well.

Senator MIKULSKI. Would you recommend that this be across all Government agencies that OPM was hit, et cetera.

Mr. SPIRES. My experience having served on the Federal CIO council and worked with many of the agencies is that OPM is not some kind of outlier here. Many Federal agencies have similar issues to what OPM faces, as far as their IT management and cybersecurity posture.

Senator MIKULSKI. Thank you very much.

Ms. Archuleta, the Federal employees, Maryland is the home to 130,000 Federal employees, and they work at everything from the National Institutes of Health to the National Security Agency. Most people at the National Security Agency are civilian employees.

What do I tell my employees, because they are quite apprehensive? What is the impact of this on them? Can you talk about this? What is the impact on them? How are you in communication? Should they be afraid that another shoe will drop, and it could drop on them and their credit ratings or whatever?

#### NOTIFICATION

Ms. ARCHULETA. Yes, and I do want to say I care very much, as you do, Vice Chairwoman, about our Federal employees. What this

breach has done is exposed their data, as you know. And I'm very concerned about that.

That is why, in terms of the first incident, we have been working hard to not only begin, but also to improve our notification system and to provide both identity theft and credit monitoring for them.

We have received much feedback from our employees. We are using that feedback.

Senator MIKULSKI. So have I. They are pretty apprehensive and agitated.

Ms. ARCHULETA. I know. I'm angry, too. I'm angry that this has even happened. I have worked very hard toward correcting decades of inattention, and I will continue to do so.

I will tell you that I'm very concerned about protecting the data of our employees, and that as we move into incident two, I am going to use their feedback, their concerns, to inform us so we can look at the wide range of options we will have available to us with these notifications.

Senator MIKULSKI. Do you have kind of a council of Federal employee organizations that you meet with that could tell you the view from the employee up, so that you really hear what they are saying?

People like myself, Senator Cardin, Senator Kaine, Senator Warner, we are very proud of the fact that the capital region is the home to so much talent that works on so many pressing national interests, from the cure for cancer to protect our country against predatory attacks. Now they are worried about predatory attacks against them.

Do you meet with them and get this advice, while we are trying to sort out the best way to have cyber shields on our dot-gov?

Ms. ARCHULETA. We are doing several things, Vice Chairwoman Mikulski. Thank you for that question.

We are working with our Chief Human Capital Officers (CHCO) Council, which are our Human Capital Officers.

Senator MIKULSKI. I don't know what Chico is. That's where I bought some of my jackets.

Ms. ARCHULETA. Mine, too.

The human capital officers for each of the agencies, as well as all of the department heads and leaders. And we have tried to adjust the notification system so it is customized to the employees.

We are also listening to our unions, our union representatives, and seeking their input, and other stakeholder groups, to see how we can better improve our notification system, not just in the long term, but during this period from June 8 to June 19, to take their feedback every day around call centers, about how we can provide Frequently Asked Questions (FAQs) on Web sites, and we could work directly with department heads and agencies, so they are assisting us in the notification process.

We take very, very seriously what we owe to our employees. I will continue to do that and to make sure that, in the second incident, we are using their input.

Senator MIKULSKI. I think that is absolutely crucial.

Mr. Chairman, I would like to really thank you also for having the IG at the table. When I chaired the committee, it was administrative procedure that all my subcommittees either had an IG come

on what were the hotspots for agencies or at least submit written testimony. The fact that you are utilizing that is really crucial.

We will have a lot to talk about this afternoon. Better talk privately.

Mr. Esser, thank you so much for your service. We so value the work of our inspectors general. They have been enormously helpful to me both as chair and vice chair of the committee to really get value for our dollar, to identify management hotspots.

And we really want to thank you for the identification not only of the problem but also the recommendation for the solutions. So thank you very much, and all of the IGs.

Mr. ESSER. You are very welcome, Senator.

Senator BOOZMAN. Thank you, Senator.

Senator Lankford.

Senator LANKFORD. Thank you.

Mr. SPIRES, let me ask you a follow-up question. You said that, coming from the CIO council before, that many Federal agencies have similar issues.

I have a twofold question. One is define what issues mean on this. And second, give me a percentage when you say "many" other agencies. Again, I'm not asking you to articulate what are the security issues and specifically where are vulnerabilities. I am not asking you to do that. Give me a guess here of how many agencies we are dealing with and what those issues are.

Mr. SPIRES. I would say many agencies of the Federal agencies have a similar kind of problem that Mr. Esser alluded to about decentralization of IT.

In and of itself, it is not necessarily a bad thing. But it has been very, very difficult for many of these agencies as they rolled out systems, and then have to support these systems, the complexity factors have grown so significantly that it is just very, very difficult for them to get their arms around systems.

I mean, at DHS, to call out DHS specifically, we would do inventories and try to, if you will, find all of the systems that we had. I think that we did a relatively good job at that. But every year, we would find more. Well, try to secure that.

I say that is the first thing, that most agencies, I believe, have that problem. I don't want to put a percentage on it, because I don't know how to measure that as far as a percentage. But I would say most of the major agencies have this problem that the CIO would not be able to sit here and say that they have a good handle on their true inventory of IT systems.

Senator LANKFORD. What about use of credentials?

Mr. SPIRES. I give a world of credit to DOD for having rolled out that Common Access Card (CAC) card years ago and having the leadership and wherewithal to make that happen. Most Government agencies are still struggling to roll out what we call the Homeland Security Presidential Directive 12 (HSPD-12) program, or the Personal Identity Verification (PIV) card, the smart card, and then use it for logical access control.

It is still an issue. If you go to the cap goals and look at where we are at, it is still an issue at most of the agencies on the civilian side.

Senator LANKFORD. Authorizations?

Mr. SPIRES. Again, I think you're hitting the hotspots here. Many systems we would find, they wouldn't have authorizations because they were out in the field and they were not under the CIO's control. Or what I also didn't like, which is kind of hiding the ball a little bit here, is you could do an interim authority to operate, and some of those would last way too long. There would be weaknesses in the systems, and it would be difficult to clear those weaknesses.

So again, I cannot put numbers on that, sir. But, hopefully, I have given you a sense of where I feel many agencies are today.

Senator LANKFORD. My question to that related to appropriations. None of those seem like big dollar items. Those are more management or current inventory, structure, process, the wonderful term of hygiene for our systems. Am I hitting that?

Mr. SPIRES. I want to be a little careful here.

Senator LANKFORD. If we have a monitor with an orange screen on it, I get it. We have some old systems out there. But I'm asking, the initial security side of this, the first rung seems to be how we are handling the information in the inventory.

Mr. SPIRES. I would agree with your sentiment that says we could manage this a lot more effectively, and we do not necessarily need new dollars to do that.

Some of the issues, though, that go to true modernization, you do need investment.

Senator LANKFORD. Sure.

Ms. Archuleta, let me ask you a question. You had in your written testimony, and in your oral testimony as well, you kind of talked through the timeline of how things went. In some areas, you were very specific of how things moved and in what order. There are a couple of terms that jumped out to me there.

Let me read this back to you. It says, "As a result of these efforts to improve our security posture, in April 2015, an intrusion that predated the adoption of these security controls affecting OPM's IT systems and data was detected by our new cybersecurity tools. OPM immediately contacted the Department of Homeland Security and Federal Bureau of Investigation."

#### INTERAGENCY NOTIFICATION

Could you give me definition of "immediately"? Is it that same day, week, month?

Ms. ARCHULETA. That same day.

Senator LANKFORD. Same day. Great.

Then you had the same issue there. You talked about the scope and impact of the intrusion. Shortly thereafter, OPM notified congressional leadership.

What is our timeframe?

Ms. ARCHULETA. We have a 7-day requirement, which we met.

Senator LANKFORD. Okay, so met it within that 7 days.

Ms. ARCHULETA. Yes.

Senator LANKFORD. Terrific. Thank you.

The contractor that was involved in this, that had responsibility for strategic IT in the security plan, who was that contractor? What were the assurances that they gave early on during the conversation in the contracting process to say we will provide security

structure, management? I'm looking for what they said they would do and what they actually did.

Who was the contractor, first?

#### CONTRACTOR SECURITY

Ms. ARCHULETA. I want to be very clear that while the adversary leveraged a compromised KeyPoint user credential to gain access to OPM's network, we don't have any evidence that would suggest that KeyPoint as a company was responsible or directly involved in the intrusion. We have not identified a pattern or material deficiency that resulted in the compromise of the credentials.

Since last year, we have been working with KeyPoint and they have taken strides in securing its network and have been proactive in meeting additional security controls that we have asked them to use to protect all of the background data.

Senator LANKFORD. So the question is then with KeyPoint, the security controls they put in now, were these security controls that were discussed earlier that were just not fulfilled, or were these things that weren't considered?

Ms. ARCHULETA. I think I understand, but let me be sure. Our detection in April discovered an intrusion into our system in late 2014. The detection was in 2015; we discovered an intrusion into our system in late 2014.

Senator LANKFORD. What I am trying to drive at is, then there were changes in security protocols. Were those changes recommended before, or are these entirely new?

Ms. ARCHULETA. They were ones we had planned and were installing as we progressed through our improvements. Unfortunately, we didn't have them in place soon enough. We are working, as I said, with a legacy system. We were testing many of our security tools. And as a result of actually being able to install this particular security tool, we were able to detect it.

Senator LANKFORD. And that plan had been in place how long?

Ms. ARCHULETA. It is part of our IT security plan, which we developed in—

Senator LANKFORD. The 2012 plan?

Ms. ARCHULETA. It is 2014.

Senator LANKFORD. Okay. Thank you.

Ms. ARCHULETA. Thank you, sir.

Senator BOOZMAN. Senator Coons.

Senator COONS. Thank you, Chairman Boozman.

Ms. Archuleta, you're in the midst of a major IT modernization project. How much do you expect that total project to cost? What elements are included in that amount?

#### OPM IT MODERNIZATION

Ms. ARCHULETA. There are four steps that we are using for that plan.

The tactical—that is, what are the tools we are going to need to protect our systems even as we move forward? We are building a new shell. It will be the platform. The third and fourth are the migration and then the disposal of the legacy system.

We are at the tactical step right now. In June of 2014, we hired a contractor to assist us in the development of the shell. We are moving toward that.

We, as I said, have identified \$67 million in 2014 and 2015 that would enable us to move toward that. We're asking for an additional \$21 million in the 2016 budget to aid us.

We are working closely with OMB to determine if another request should be made.

Senator COONS. Has a major IT business case been prepared as OMB requires for IT projects?

Ms. ARCHULETA. Yes, it has. We worked very close with OMB. This is one of the points that the IG brought out in his flash audit. I can assure the IG that we, in fact, have been working very, very closely with OMB.

This is an urgent issue. We are moving as fast as we can, making sure that we track, we justify and document all that we are doing consistent with the OMB standards that have been given to us.

We have a budget that we worked very closely with OMB to deliver.

Senator COONS. In response to the IG audit, one of the concerns was why you would give a sole-source contract, if I understand correctly, to a single contractor to manage all four phases of this very large project.

What type of contract is it? Is it a fixed-cost project? What steps are you considering in light of the audit?

#### OPM CONTRACTING

Ms. ARCHULETA. As I said before, there are oftentimes places where we have areas of agreement and areas where we would like to have further consideration with the auditor.

In his flash audit, the inspector general encouraged the use of either existing contracts or the use of full and open competition. I would like to assure you and the inspector general that the processes followed in awarding the already existing contracts have been perfectly legal, and that we will continue to ensure that any further contracts and processes entered into will also be perfectly legal.

He also expressed concern that the sole source contract used in the tactical and shell phases should not be used for migration and the cleanup phases that I described earlier. I understand his concerns. I would like to remind the inspector general that the contracts for migration and cleanup have not yet been awarded.

Where we would like to have further discussion with the inspector general is the timeline, the practical timeline, for our major IT business case. He is suggesting that we move that out to fiscal year 2017. I would like to move that much quicker, given what we have already experienced.

I assure the inspector general and everyone here that all of our decisions are being tracked, documented, and justified.

He has made a number of recommendations regarding contracting and standards that rely on external sources for assistance, and I believe the Federal Government and through the good work that Tony Scott is providing to us and all of our partners in Gov-

ernment have strong solutions to offer. I am going to look forward to talking more to him about his suggestion.

Senator COONS. Have you had a chance to look at other agencies that have had successful IT projects to use as a model? As you mentioned, have you some sources of valuable insight into how to manage multi or multiphase expensive and time-critical IT projects.

Have you looked at whether having an outsider contractor managing the project or breaking it into more bite-size pieces might achieve some of your goals?

Ms. ARCHULETA. Well, we are looking at all of our options, certainly. This is a very serious issue. I am taking it very seriously and looking to all of the resources I have available to me. I will, certainly, do that.

I believe that the Federal CIO is an important asset to us, as are our partners at the Department of Homeland Security, National Security Agency, and the Federal Bureau of Investigation. So we are looking to those. And I welcome the Inspector General's suggestions. And as I move forward through this process, I will be listening to him carefully, as well as my partners across the Government.

Senator COONS. I appreciate that response.

Mr. Spires, you were the former CIO at DHS and IRS, both of which have had very cumbersome, difficult, and often challenged IT projects. Were you able to do turnaround on some of the legacy IT failures there? What advice do you have for OPM, as they engage in another expensive, complex, multiyear modernization effort?

Mr. SPIRES. Sure. First, I would make the note that it is always about a team effort, in order to deliver these kinds of programs. I actually joined IRS and took over the modernization program. At the time, it was on the GAO high-risk list, and I am pleased to say that, as a team effort, it took a long time, but we were able to improve our processes to the point where recently that program was removed from the high-risk list, which is quite an accomplishment.

Let me just say that I have reviewed many programs. We could have a long discussion about how to appropriately manage IT programs. I will make a couple of points very quickly.

One thing that is very critical is the overall governance framework that you put in place. You need to get the right stakeholders in the room to work together to make this happen. All too often in Government, I have seen issues where that does not happen.

The other thing I would say is don't over-rely on contractors. You need to have a program management office of Government officials that have the requisite experience and skill set to be able to run these programs.

And I'm not picking on OPM. I don't know much about their modernizations at all. But I have found the smaller agencies, I think, struggle more with this because they do not have the heritage of having learned those lessons within the agencies themselves.

Senator COONS. Thank you. I see my time has expired.

Mr. Spires, Mr. Esser, Ms. Archuleta, thank you for your testimony today.

I'm grateful for the input of the IG and for your offer to continue to work with us and consult with us as we move forward to try to

offer critically needed reassurances, particularly to law enforcement, but all Federal employees, and to find timely and cost-effective solutions to this and other cyber challenges.

Senator BOOZMAN. Senator Moran.

Senator MORAN. Chairman, thank you very much.

Mr. Spires, based upon what you heard today, your knowledge of Government agencies and their cybersecurity issues, is this a management issue or is this a resource issue?

Mr. SPIRES. It is more of a management issue, sir.

Senator MORAN. Why do you say that?

Mr. SPIRES. Because of the dispersed nature of the way IT has been run in a lot of agencies, there are so many let's say inefficiencies that have crept into the system that I don't believe we effectively spend the IT dollars we receive.

So I believe with the proper drive towards management, you can actually drive a lot of savings from the existing budgets. But caveat that. When you are talking about new modernization programs, sometimes with the right business case, it does make sense to invest in those.

Senator MORAN. Based on your response to Senator Coons, I assume there is a natural inclination when these issues arise that the easy thing to do is to hire a contractor. Within the agency, we do not know this stuff, it is not our primary mission, let's just get somebody in here who takes care of this.

This committee, when Senator Udall was its chairman, we worked on FITARA and issues related to how to improve the role CIOs play in an agency, in part trying to compensate for, I think, an attitude that we are not tech folks, somebody else is responsible for that.

Ms. Archuleta, describe to me how you work with your CIO. Let me ask a question first about this.

The first breach I think you were aware of goes back to June 2014. As I recall, you and others testified in front of this committee in May of 2014, and the following month, June, OPM became aware of a breach.

#### TIMELINE OF BREACHES

Ms. ARCHULETA. Yes. The first breach that we discussed with you was—

Senator MORAN. I don't think you discussed this in May. If you knew about it, I do not think we knew about it.

Ms. ARCHULETA. Okay. I'm sorry, sir.

I want to look and make sure I have my months right. March 2014 was when we identified some adversarial activity. But there was no PII that was lost in that.

In June 2014, which is what you may be referring to, USIS was breached. There was OPM data that was compromised. It impacted about 2,600 individuals.

In August of 2014, KeyPoint Government solutions, was breached. That breach compromised approximately 49,000 individuals.

In April of 2015 was the breach that I described earlier, as well as the one in May.

Senator MORAN. So let me make sure I understand what you just said. There were three breaches that occurred prior to the two that we are now talking about.

Ms. ARCHULETA. There was the OPM network in March, June of 2014 USIS, in August KeyPoint.

Senator MORAN. What changed at OPM? You obviously then became aware on three occasions somebody is trying to intrude on our system. What then did OPM do after realizing that?

#### OPM IT MODERNIZATION

Ms. ARCHULETA. If I could just go back a little bit, because I want to reassure you, to my colleague's point, that one of the first actions I took as OPM director was to hire Donna Seymour. The second action I took was to develop an IT strategic plan that had exactly the pillars my colleagues describe.

So for IT leadership, look to OPM's CIO. IT governance is my whole leadership team we must buy into the design and the structure of the IT plan and its development. And for IT architecture, what was it going to take for us to build out the systems that we needed, in view of our legacy system?

Regarding IT data, we needed to be informed. We needed to know that what we were doing was right and that we were doing this in a way that was analytical. We also had as an important pillar IT security, obviously very, very important. As we were building out, even as we were working on our strategic plan, one of the most important pillars was IT security.

Since Donna Seymour came in as CIO, and because of her experience, and as Mr. Spires says, the experience we have in Government, we brought her from the Department of Defense and the Department of Transportation, that she was able to apply those skills and that talent to identifying not only what our strategic steps are but how we could begin to develop them.

The first thing we needed to look at was what we could place on that legacy system, and what would it take to do that?

That is where she has begun and what she continues to do throughout her tenure.

Senator MORAN. Your point is, not necessarily following the three breaches that we just talked about, but from your arrival, your priority was to get a CIO and begin implementation of a plan?

#### OPM IT STRATEGIC PLAN

Ms. ARCHULETA. I will tell you, Senator, that from the first time I was briefed on our IT infrastructure during my confirmation preparation, I knew that there was a problem. And that is why, in my confirmation hearing, I said it would be a top priority, and I promised your colleagues that I would develop an IT strategic plan, which I did, and produce within the first 100 days. I was also wise enough to hire Donna Seymour.

Senator MORAN. The IT strategic plan that you just mentioned, is that something we could see?

Ms. ARCHULETA. Absolutely, sir. It is on our Web site. I will make sure you get a hard copy as soon as possible.

Senator MORAN. Mr. Chairman, let me see if I have additional follow-up.

Following that IT strategic plan, is there a new plan as a result? It is just implementing this one?

Ms. ARCHULETA. As you know, a plan is dynamic, and as we learn things, that plan changes. But we are following it. We are making sure every component—governance, leadership—making sure that we’re making sound decisions on the architecture, that we are building and making sure it is based on clear analytics, and that cybersecurity is an important component of all of that.

Senator MORAN. Are there benchmarks that are now in place within that plan so that we see whether we are making progress, benchmark by benchmark?

Ms. ARCHULETA. I would like to come back to you and show you what those benchmarks are, sir.

Senator MORAN. Okay.

Let me ask about notification. You indicated in your testimony, and I wrote this down as well, “as soon as practicable.” And I understand the value of that phrase.

The President’s proposed legislation for notification to occur within 30 days of a breach, how do you think practicable fits with the 30-day requirement?

Ms. ARCHULETA. Within the proposed legislation, “practicable” is included in there. I can assure you we are trying to do everything we can to come as close to that date as we possibly can.

Senator MORAN. All right.

Is there anyone who oversees IT security outside of OPM? What is the relationship with OMB?

Ms. ARCHULETA. It is a very close relationship. We work very closely with the Federal CIO who has responsibility for this, Tony Scott. He has been at OMB for about 90 days now. He has been engaged with us from the very beginning. He and Donna have a strong relationship, and he has a strong adviser role to us.

Senator MORAN. Prior to his arrival 90 days ago, was there someone filling that responsibility as well?

Ms. ARCHULETA. I don’t know that, sir, but I would be glad to get that information back to you.

Senator MORAN. Okay. Thank you very much.

Ms. ARCHULETA. Thank you, sir.

Senator BOOZMAN. Thank you, Senator Moran.

Thank you all for being here. Again, I apologize for the earlier delay. This is such an important hearing. I think this is one of the most important hearings we will have this year. We will be following up in the not-too-distant future, again making sure things are moving in the right direction.

I want to thank you all for participating. I also want to thank my staff and Senator Coons’ staff for the excellent job they have done in preparing for the hearing.

At this time, I ask unanimous consent that statements by the National Treasury Employees Union and the Government Employees AFL–CIO be included in the hearing record.

[The information follows:]

## PREPARED STATEMENT OF THE NATIONAL TREASURY EMPLOYEES UNION

Colleen M. Kelley, National President

Chairman Boozman, Ranking Member Coons and distinguished members of the subcommittee, I would like to thank you for the opportunity to share our members' perspectives on the recent announcements of agency data breaches impacting Federal employees. I commend you for holding this hearing on an extremely urgent issue for the Federal workforce. As President of the National Treasury Employees Union (NTEU), I have the honor of representing over 150,000 Federal workers in 31 agencies.

Mr. Chairman, as you can imagine, there is great fear and outrage on the part of Federal employees and retirees in the wake of the U.S. Office of Personnel Management's (OPM) announcements on June 4, and more recently on June 12, that millions of current and former Federal employees may have had personally identifiable information (PII) compromised owing to breaches in databases containing various personnel records. Federal employees have had a difficult few years, facing multi-year pay freezes, furloughs, sequestration, and this type of exposure of personal information is the final straw. Such exposure is simply unacceptable.

It is important to note that these breaches follow wide-scale breaches of health insurance carriers earlier this year that included Federal employees enrolled in several Federal Employees Health Benefits Program (FEHBP) plans, and multiple announcements of agency breaches in 2014 affecting background investigation and suitability records. Federal employees are required to provide significant amounts of personal data to their employing agencies, for general employment purposes, as well as for suitability and security clearance purposes. NTEU asks that this subcommittee act to ensure that agencies have the ability to immediately safeguard Federal employees' information going forward. It should come as no surprise that employees are questioning the idea of submitting this type of detailed personal information to their agencies in the future, and are particularly pointing to the suitability and security clearance process, forms, and storage as areas that need to be immediately changed. We also ask the subcommittee to keep these breaches in mind as serious consideration of so-called "Continuous Evaluation" (CE) policies move forward in the security clearance and suitability reform areas, as well as for oversight purposes of the Administration's Insider Threat program.

At the moment, a principal outstanding concern for Federal employees and retirees is the confusion about what exact type of individual data and information was in fact compromised, and of whom. In its first statements, OPM confirmed that a breach had potentially compromised names, dates and places of birth, Social Security numbers, and addresses. However, a multitude of media and other public statements followed maintaining that the exposure was far greater in number and the information even more intrusive—that the type of information that may have been accessed by outsiders involved information about family members, beneficiary information from employee benefit programs, bank accounts, data submitted and stored from Declarations of Federal Employment and Standard Forms 85 and 86<sup>1</sup> (among others) as part of routine background investigations, including detailed financial information and medical history, home addresses and other PII and data for annuitants. Late on June 12, OPM informed NTEU that this was indeed the case—that the worst case scenario for individuals' privacy—be they Federal civilians, military personnel, contractors or other individuals simply appearing in various documents, and our Nation's national security has occurred. However, NTEU wants to be clear that which employees have been affected by this apparent wider, and more serious breach, is still unknown to us and most importantly to the affected individuals.

OPM's statements issued to us and to agency heads still do not contain any information about whether individuals who do not possess security clearances, but who provide detailed information for suitability determinations and Standard Form 85 for critical non-sensitive positions, are also included in this breach. Not knowing whose data, and what exactly has been accessed and compromised, is creating widespread confusion and anxiety, on top of the general frustration of having one's personal information compromised be it from a foreign power, a thief, or otherwise ill-intended individual. Employees deserve to know what exact databases and information was hacked, and they need to be in a position to act, given the high level of risk they and their families are facing. It will also be important to address whether spouses, siblings, and other relatives, as well as former non-Federal coworkers and acquaintances whose PII and contact information is provided, also had their information compromised, and whether there are plans to notify these members of the

<sup>1</sup> Questionnaires for Public Trust, Non-Sensitive, and National Security Positions.

public, and to provide them with credit and identity protection services. We do not currently have any notification details to share with our members concerning the latest news from OPM, which again is unacceptable. I ask this subcommittee to ensure that the notification plan for all of these affected individuals is made public, and that it is put into action immediately.

Given that more than a week has passed since this wider breach was announced, NTEU believes it is time to immediately extend blanket credit monitoring and identity theft protection services to the entire Federal workforce. We understand that the forensic investigation may take time, and that there are serious national security implications to this breach, so in order to best protect employees going forward, a blanket extension is needed. Since large numbers of employees (OPM estimates 2.1 million) have just received these services as part of the first OPM reported breach, it should be a relatively small number of additional employees who need this coverage extended to them.

OPM responded positively to NTEU's initial request that Federal employees be allowed to use Government computers in order to be able to contact CSID, the OPM-selected contractor, for credit monitoring purposes and to enroll in the identity theft protection services. Additionally, OPM also acted on NTEU's request to ensure access to Government computers for those employees who do not regularly use computers on the job. While OPM has encouraged agencies to do these things, NTEU urges agency heads and this subcommittee to ensure that this access is indeed granted.

It is critically important for employees and retirees to be able to access and enroll in protection services as soon as possible. While NTEU is aware that OPM's contractor-provided notifications have begun to be emailed and mailed directly to active employees for the first breach, we are aware of various difficulties that may exist in reaching affected annuitants and former employees, whose mailing addresses are not actively maintained by employing agencies or OPM. Additionally, many of our members are reporting extensive problems when attempting to enroll in the CSID-provided services—ranging from not being able to reach an operator on the toll-free line, to the Web site crashing or freezing when they are attempting to enter the required enrollment information, to the rejection of assigned pin numbers and passwords, to the inability to establish required connectivity to the CSID Web site, to official email notifications going into spam filters, and to family members receiving the employee's notification letter, at an address that the employee has never lived at, or used for any purpose. In short, the CSID notification and enrollment process has been a disaster for many NTEU members.

A major concern for employees is the delay in notification from the time of the actual discovery of the breaches. It is imperative that affected individuals receive swift notification of any type of breach compromising PII and other information. Any delay in notification only increases the likelihood of individuals experiencing identity theft and suffering financially. As you know, Mr. Chairman, NTEU represents employees at U.S. Customs and Border Protection (CBP), and in September 2014, the Department of Homeland Security (DHS) became aware of a breach involving KeyPoint, a contractor providing background investigations and support. The overall volume and sensitive type of information that is provided by employees undergoing a background investigation—either as a new hire or for a periodic reinvestigation—is significant, and includes extremely personal details of employees, their family members, and of their friends, and even of their coworkers and acquaintances. However, it was not until June 4, 2015 that DHS began providing and notifying CBP employees of their ability to enroll in credit monitoring and identity theft protection services. A nine month delay is simply unacceptable for all individuals involved. Moreover, two simultaneous, ongoing employee notification processes of compromised employee personnel records at CBP is leading, not surprisingly, to major confusion in the workplace.

Mr. Chairman, I also want to share that I have requested that, as we move forward, serious consideration be given by the administration to providing both the credit monitoring services and the identity theft protection services for a significantly extended period of time beyond the current 18 months. Given how long these breaches may have gone undetected, and since the exact identities and data compromised is not yet known, NTEU believes these items to be prudent courses of action. As an example, following this year's Blue Cross Blue Shield healthcare breaches, carriers provided 24 months of protective services to affected enrollees. Additionally, we ask that blanket coverage be provided now to those individuals affected in the second breach. Serious compromises of data and personal information demand serious responses from the U.S. Government for the protection of its most valuable asset, its people.

I again thank the subcommittee for the opportunity to provide NTEU's views on these alarming employee data breaches, and for your work to identify the source of these intrusions, as well as to identify the compromised employee records and personal information. And, most importantly to help ensure that this does not happen again. However, for the information already compromised, time is of the essence, and clear guidance and immediate notification, with adequate levels of protection, is warranted. Ultimately, NTEU members want to be assured that their information, and their family members' information, is not at risk because of their profession. Our members deserve to be able to trust that the Government can properly secure their private information.

---

PREPARED STATEMENT OF THE AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES,  
AFL-CIO

OPM INFORMATION TECHNOLOGY SPENDING AND DATA SECURITY

Chairman Boozman, Ranking Member Coons, the American Federation of Government Employees, AFL-CIO (AFGE) which represents more than 670,000 Federal employees, would like to thank the subcommittee for holding this important hearing on the recent data breaches to the Office of Personnel Management's electronic employee data systems. Unfortunately, in the days since the breach was originally announced, the number of individuals who are or have been employed by the Federal Government, and potentially had their personal data hacked continues to increase. Very little substantive information has been shared with Federal employees, despite AFGE's numerous requests for specific information in an effort to help those affected by the data breach. All individuals affected by the OPM data breach deserve nothing less than a clear path forward that allows them to take immediate action to protect themselves from the misuse of their stolen personal information, successfully monitor their credit, and continue their work as Federal employees with confidence that the necessary precautions will finally be taken to protect their personal data.

OPM must commit to answering the most basic of questions regarding the breach. The fact that OPM continues to refuse to answer simple questions about the dimensions of the breach have made the Federal and DC Government employees and retirees that AFGE represents deeply skeptical of any information coming from OPM. AFGE understands the sensitive nature of the current criminal investigation that is underway, however, there are some questions and issues that the agency has a moral responsibility to answer. For example, one question that still has not been adequately addressed by OPM is whether or not the data that was stolen can be linked to Federal employees' bank accounts or direct deposit information. Federal employees deserve answers to all of their questions so they can take appropriate action.

Based on the information that OPM has provided, AFGE believes that the Central Personnel Data File was the targeted database, and the hackers are now in possession of all personnel data for every Federal employee, every Federal retiree, up to one million former Federal employees, as well as similar data for their family members. We believe that hackers have every affected person's Social Security number(s), military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance, and pension information; age, gender, race, union status, and more. In fact, at the House of Representatives Oversight and Government Reform hearing held on June 16, 2015, OPM Director Katherine Archuleta testified that Federal employees' Social Security numbers were not encrypted, and thus were compromised. This is a cyber-security failure that is absolutely indefensible and outrageous. While OPM has informed Federal employees that they will provide 18 months of credit monitoring and \$1 million in liability insurance, AFGE believes that a mere 18 months of credit monitoring is entirely inadequate, either as compensation or protection from harm. Federal employees will suffer the consequences of the OPM data breach far longer than 18 months. In order to protect the personal data of the millions of individuals affected by the data breach from this point forward, OPM owes employees and their family members free lifetime credit monitoring and liability insurance that covers the entirety of any loss attributable to the breach. With the personal information of millions of people stolen, we cannot underestimate the long-term threats to Federal employees' personal finances, credit, and physical safety.

AFGE also requests that OPM reconsider the decision to enter into contact with Winvale/CSID, a contractor given responsibility for answering affected employees' questions involving their stolen personal information. Based on our membership

feedback, Federal employees have not been able to speak with an actual person when they have questions. At the very least, the terms of the contract should have included guaranteed access to points of contact that can answer specific, personal questions that affected Federal employees may have regarding the data breach. Federal employees who have been victimized by this breach deserve more than a Web site that is difficult to navigate and call center contractors who do not know the answers to questions that go beyond a Frequently Asked Questions (FAQ) template. Those affected should have access to OPM employees who can respond to questions that are unique to their individual situations.

AFGE has also received numerous complaints from Federal employees who describe their horrendous experience trying to access assistance from the contractor hired to perform credit monitoring. These complaints range from reports of the Web site constantly crashing to the information the contractor produces being inaccurate and out of date. A recent report on Federal News Radio noted, CSID is “. . . thought of as a company that helps others get on the General Services Administration (GSA) schedules, prepare proposals and the like, and their GSA schedules are for things such as lab equipment and IT software services, but there is nothing about credit monitoring, insurance or similar offerings . . . interestingly enough Winvale’s Web site now says they provide credit monitoring services, but their profile on Bloomberg does not mention it at all.”<sup>1</sup>

Accuracy and accessibility are the entirety of the service that Winvale/CSID is supposed to be providing. Thus far, Federal employees have not been able to rely on the accuracy and accessibility of the credit monitoring services that have been provided. Yet, OPM gave Winvale/CSID what appears to be a sole-source \$20 million contract with four 1 year renewal options. These issues need to be addressed and Federal employees must have reliable credit monitoring services immediately.

AFGE has received disturbing reports that agencies are denying Federal employees the time to deal with the impact of the data breach. At numerous agencies, employees are forbidden to use their government computers for any purpose other than a work assignment. They are forbidden from using their government computers to access personal emails or any non-work related Web sites for any reason. Federal employees dealing with this breach need to be able to visit their banks, Social Security offices, mortgage holder’s offices, the management offices of their apartment complexes, and other creditors in order to deal with the fallout of having to change credit card and bank account information. Many agencies’ computer firewalls prevent employees from being able to handle these kinds of transactions online. Therefore, agencies should grant employees time during normal business hours to take preventive measures such as contacting their financial institutions and businesses as notification of their current situation. Additionally, it is extremely important that OPM ensure that agencies are meeting all of their collective bargaining obligations on procedures for accommodating employees trying to deal with the breach.

Federal employees trusted OPM with their personal information and the agency failed them. Their personal information was not properly guarded, and as a result, Federal Government workers and their families must now live with the threat of having the most intimate details of their lives exposed, and illegally used against them. The Government must now earn back the trust of these employees and future public servants. AFGE thanks the subcommittee for holding this hearing.

#### ADDITIONAL COMMITTEE QUESTIONS

Senator BOOZMAN. If there are no further questions, the hearing record will remain open until next Tuesday, June 30, at noon, for subcommittee members to submit any statements or questions to the witnesses for the record.

[The following questions were not asked at the hearing, but were submitted to the Agency for response subsequent to the hearing:]

<sup>1</sup> Federal News Radio, *OPM Contract for Credit Monitoring Services Called Into Question*; <http://www.Federalnewsradio.com/520/3875508/OPM-contract-for-credit-monitoring-services-called-into-question>.

## QUESTIONS SUBMITTED TO KATHERINE L. ARCHULETA

## QUESTIONS SUBMITTED BY SENATOR JERRY MORAN

## DATA BREACH

*Question.* At last week's hearing, you indicated that OPM estimated the total number of individual impacted by this most recent data breach to be approximately 4 million. Media reports suggest that an internal memo from OPM suggests that as many as 18 to 30 million individuals could be impacted by the series of breaches dating from March 2014 until present. Can you please provide the most up-to-date information regarding the number of individuals impacted directly by this breach? What percentage of the total number of OPM's records are considered to contain national security information or sensitive information necessary for identity theft or fraud? Of that, what percentage of those records were included in this breach? In addition, please provide any information you see fit that can be helpful to quantify the severity of this breach.

*Answer.* In April 2015, OPM discovered that the personnel data of 4.2 million current and former Federal Government employees had been stolen. This means information such as full name, birth date, home address, and Social Security Numbers were affected. This number has not changed since it was announced by OPM in early June, and individuals who were affected should have already received a notification.

While investigating this incident, in early June 2015 OPM discovered a separate but related incident where additional information had been compromised, including background investigation records of current, former, and prospective Federal employees and contractors. OPM and the interagency incident response team have concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants. Some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. Notifications for this incident have not yet begun.

*Question.* You indicated in your testimony last Tuesday that there were three separate breach incidences that caught the attention of OPM last year. In March 2014, you explained that OPM successfully detected a breach attempt but that no personal information had been obtained. Later that summer, two government security clearance contractors were breached. In June 2014, 25,000 records, which included highly-sensitive security clearance information, were obtained from security contractor U.S. Investigations Services (USIS). Two months later, another security clearance contractor, KeyPoint Government Solutions, suffered an even greater breach. This time over 48,000 records were obtained. In each successful breach incidence, OPM was required to issue notification letters to affected individuals. OPM clearly knew that this sensitive security clearance information was a target of hackers. It was later revealed that this sensitive information may have been used to infiltrate the OPM network. Was this security clearance information used to gain access to the OPM network? Please offer a detailed description of your response to these serious breaches. What security procedures and improvements were put in place? How often did you meet with your CIO and other top security officials within OPM to discuss these breaches and develop a response strategy? Please provide a calendar of those meetings and the topics discussed. Please describe any new policies OPM required to access the OPM network following the breaches.

*Answer.* The adversary gained access to OPM systems through the agency's Local Area Network by employing stolen user credentials from a contractor. OPM has already taken a series of 23 concrete steps to improve information security, as outlined in its recent Cybersecurity Action Report. These include:

- Implementing two factor strong authentication for all privileged users, and increasing the percentage of unprivileged users with two factor Strong Authentication;
- Restricting remote access for network administrators and restricting network administration functions that can be performed remotely;
- Reviewing all Internet connections to ensure that only legitimate business activities have access to the Internet;
- Deploying new hardware and software tools, including 14 essential tools to secure the network;

- Deploying anti-malware software tools across the environment to protect against cybercrime activities that could compromise the agency's networks;
- Establishing a 24/7 Security Operations Center, staffed by certified professionals, to monitor the network for security alerts;
- Implementing continuous monitoring to enhance the ability to identify and respond, in real time or near real time, to cyber threats;
- Installing more firewalls that allow the agency to filter network traffic more effectively;
- Working with the intelligence community and other stakeholders to identify high value cyber targets within the OPM network where bulk PII data are present, and mitigate the vulnerabilities of those targets to the extent practicable;
- Modernizing OPM's IT network technology and architecture; and
- Tightening policies and practices for privileged users.

These actions have put OPM in a much stronger and more secure posture than it was when then-Director Archuleta assumed her role. OPM systems currently thwart millions of intrusion attempts that target its networks every month. In addition to these past and ongoing activities, OPM has recently identified several additional actions to bolster its security and modernize IT systems. These include:

- Deploying two factor Strong Authentication for all unprivileged users (Complete);
- Expanding continuous monitoring and completing implementation of the Continuous Diagnostics and Mitigation program by March 2016;
- Establishing requirements for future contracts, as appropriate, to ensure access to contractor systems in the event of an incident (Complete);
- Completing a review of encryption of databases (Complete);
- Hiring a new cybersecurity advisor (In progress);
- Consulting with outside technology and cybersecurity experts to identify further steps the agency can take to protect its systems and information (Complete);
- Migrating to a new IT environment capable of significantly increased security controls (In progress); and
- Establishing regular employee and contractor training on appropriate cyber hygiene and practices (In progress).

*Question.* In December 2014, one of the breached security contractors, U.S. Investigations Services (USIS) has accused the OPM of neglecting to share information that might have helped the contractor detect the breach that occurred in June 2014. Did OPM reveal to its contractor, USIS, that it had recently suffered a cyberattack? If not, why did OPM not share this information? To what extent did OPM's continued refusal to adopt IT best practices and OMB-required IT procedures contribute to these potential security vulnerabilities at the contractor level? Was it required that OPM share critical information about the March 2014 attack?

*Answer.* OPM did not disclose to USIS that OPM systems had been breached in March 2014. In our opinion, there was no clear requirement that OPM notify USIS of the breach.

*Question.* One significant factor that may have led to this breach is the repeatedly ignorance of OMB policies and IT best practices. As Assistant Inspector General Esser indicated in testimony, the fiscal year 2014 FISMA report offered OPM 29 recommendations covering a wide variety of IT security topics; however, OPM has only adopted 3 of those 29 recommendations to date. The fiscal year 2014 audit also revealed that 11 of 47 OPM IT systems were operating without a valid Authorization, including some of the most critical and sensitive applications owned by the agency. One tool available to OPM is the ability to institute administrative sanctions to correct this gross negligence. The OIG explains this could be an effective way to reduce non-compliance with FISMA requirements.

*Answer.* Within the past year OPM has taken great strides in improving the enterprise. Much of the recommendations issued by DHS in 2014 have been achieved and OPM is on track to meet or exceed all Federal mandates including leading in the FISMA Cyberstat, DHS TIC v2, and HSPD-12.

The following are some of the accomplishments:

- Implemented Level 4 two factor authentication for all privileged and non-privileged users. The requirement of utilizing PIV for all users has made OPM a leader in complying with the HSPD-12 mandate and significantly reduces the attack surface of the network.
- Restricted remote access for network administrators and restricted network administration functions that can be performed remotely.

- Reviewed all connections and associated Access Control Lists (ACLs) to ensure only legitimate business connections have access to the Internet. This includes blocking privileged users' access to the Internet.
- Required administrators to authenticate through a privileged user management appliance in order to perform all administrative functions. Direct access to servers or databases cannot be achieved by users or administrators.
- Deployed new hardware and software tools to secure the network. Including:
  - Endpoint protection to detect and prevent malicious and unauthorized software from installing and running on endpoints and servers.
  - Web Application Firewalls to monitor traffic to and from Web applications and prevent common attacks such as DDOS, cross-site scripting, SQL injection, and session hijacking.
  - Endpoint anti-virus/malware scanning to quickly detect and block viruses and malware.
  - Automated threat response to unify, automate, and orchestrate incident responses to ensure speed and decisiveness.
  - Network Access Control to detect and limit unauthorized access from devices that do not meet OPM policy.
  - Business critical data and database compliance by providing visibility into data access and tracking users' activity and data sets.
  - Advanced firewall services to better protect and filter network traffic on the internal and external perimeter.
  - Network risk and vulnerability monitoring and assessments to identify areas of weakness in the network architecture.
  - Inbound and outbound SSL inspection to audit and monitor encrypted malicious traffic.
  - Deployed network and email data loss prevention solution to detect data exfiltration.
  - Implemented anti-phishing and anti-malware inspection and prevention of email traffic.
- Deployed additional firewalls to segment and monitor internal traffic.
- Implemented continuous monitoring to enhance the ability to identify and respond, in real time or near real time, to cyber threats.
- Centralized security management and accountability into the Office of the CIO and staffed it with security professionals who are fully trained and dedicated to information security on a full-time basis.
- Conducted a comprehensive review of IT security clauses in contracts to ensure that the appropriate oversight and protocols are in place.

*Question.* A number of current and former Federal employees have expressed confusion and concern about the credit monitoring process, which requires the input of sensitive information online. These workers have also complained about frustrating multi-hour wait times to speak with CSID representatives on the phone. Many are unfamiliar with the vender, CSID, and the process to enroll in credit monitoring services. What assurances can you provide that the information submitted by impacted individuals will be safe and secure with this contractor? Does this contractor use secure technologies, such as encryption, to protect sensitive information? Are you aware of any phishing attacks or other scams to obtain sensitive information from impacted individuals? Has the contractor made a commitment to improve wait times or increase their ability to address claims being made by impacted individuals?

*Answer.* CSID is the engine behind eight of the top 10 identity theft protection companies. CSID fully encrypts critical values in production databases to prevent the exposure of sensitive information stored in the database to unauthorized persons. CSID employs policies, procedures, and protection standards meeting or exceeding those in the industry for securing Personal Identifiable Information (PII). CSID is required to comply with standards around data, systems, process, and personnel resources consistent with the same standards held for all three credit bureaus. The contract provides that OPM may conduct onsite inspections—see clause 15.31 1752.239–86 Contractor System Oversight/Compliance (Sep 2014). CSID is subjected to regular vulnerability scans, penetration tests, annual PCI audits, credit bureau audits, and other security related exercises that allow CSID to meet these compliance standards. OPM's contract with Winvale includes additional clauses regarding the Privacy Act and other matters involving sensitive information processing and storage. With any publicly announced data breach there are attempts by bad actors to exploit the situation. OPM has gone to extensive lengths via our Web site and guidelines issued to agencies to provide tools for affected individuals to validate communications. CSID, in communication with OPM, has added significant

numbers of trained staff to their call centers, and the average wait time is now less than one minute.

*Question.* Earlier this year, an American healthcare company suffered a massive breach that involved roughly 80 million records. In that instance, the company decided to provide 24 months of credit monitoring services. Why did OPM choose to offer 18 months of credit monitoring services to impacted individuals? What is the total estimated cost to provide both breach notification and credit monitoring services to 4 million figure you provided as the number of impacted individuals? What would be the cost to provide breach notification and credit monitoring services to 18 million impacted individuals, as has been the number suggested in media reports this week?

*Answer.* A careful and thoughtful analysis of the risks presented by the personnel records incident as well as a review of the services available, precedent, and industry best practices led OPM to conclude that 18 months is the appropriate duration for the comprehensive suite of services offered to help Federal employees.

*Question.* During your testimony, you mentioned the development of an OPM IT plan that was drafted within the first 100 days of your tenure at the agency. Will you please share that plan? What elements of the plan outlined OPM's timeline for securing sensitive personnel data?

*Answer.* A copy of the OPM Strategic IT Plan was sent to your subcommittee. The Information Security section (page 17) details three phases that ensure our information security policies are rigorous and cost effective based on a risk assessment methodology that considers both current and potential threats.

*Question.* One of the witnesses at last Tuesday's hearing testified that the most important thing OPM could do is secure sensitive information immediately. How does OPM plan to develop this capability? Does OPM plan to build its own security tools? To what extent has OPM either requested proposals for commercially available security software or tools?

*Answer.* OPM continues to take aggressive action to strengthen its broader cyber defenses and IT systems. As outlined in its recent Cybersecurity Action Report, in June, OPM identified 15 new steps to improve security, work with outside experts, modernize its system, and ensure accountability. OPM is currently completing a comprehensive review of its IT systems to find and address any potential vulnerabilities. It is bringing in experts from in and outside of the Government to help with these efforts, including a new cybersecurity advisor. OPM is also working with interagency partners on a review of key questions related to information technology governance, policy, security, and other aspects of the security clearance process, including where such data should be housed in the future.

#### INFORMATION TECHNOLOGY GOVERNANCE

*Question.* Describe the role of your agency's Chief Information Officer (CIO) in the development and oversight of the IT budget for your agency. How is the CIO involved in the decision to make an IT investment, determine its scope, oversee its contract, and oversee continued operation and maintenance? How often do you meet with your CIO and other top IT security professionals within your agency? Please provide a detailed summary of meetings you have had with your CIO and her team since you entered the agency in November 2013.

*Answer.* The CIO is involved in every aspect the IT budget development process at OPM. The OPM CIO is responsible for all major IT investments from scoping to oversight of the delivery of services on a contract. The CIO discusses these decisions through standing weekly, and sometimes daily, meetings with the OPM Director.

*Question.* What formal or informal mechanisms exist in your agency to ensure coordination and alignment within the CXO community (i.e., the Chief Information Officer, the Chief Acquisition Officer, the Chief Finance Officer, the Chief Human Capital Officer, and so on)?

*Answer.* The Chief Operating Officer serves as a leader in OPM to focus the efforts of the CXO positions. Each of these interests is represented in OPM's strategic plan as a supporting function to the primary business missions of OPM. The OPM strategic plan addresses the priorities of the agency and ensures alignment of resources toward the stated goals. The COO hosts a weekly staff meeting so CXO executives can share ideas, work through challenges, and determine the best way forward for OPM.

*Question.* According to the statistics from your office, 46 percent of the more than 80,000 Federal IT workers are 50 years of age or older and more than 10 percent are 60 or older. Just 4 percent of the Federal IT workforce is under 30 years of age. Does the makeup of your agency reflect such demographic imbalances? How is OPM addressing this talent issue?

Answer. Our objective, given the current fiscal environment, is to raise and leverage awareness of the Federal cybersecurity workforce across Government. This includes ensuring that the public knows these positions are available and how to apply for them.

- This awareness is being done primarily by working with technology departments at colleges and universities to educate students and staff about the Pathways Program and the hiring flexibilities available to agencies to recruit and onboard STEM graduates.
- The Presidential Management Fellowship (PMF) program and the new PMF-STEM portfolio attract applicants with cybersecurity skills in disciplines such as computer science, computer engineering and computational analytics.
- Our outreach guidance provides Federal agencies with up-to date information on how to message their opportunities, encourages them to work within their communities to strengthen the local talent pipeline in their communities, and provides workforce planning tools that enable them to plan for and get the workforce they need.

OPM also has the leadership role for the Administration's Initiative to Close Cybersecurity Skill Gaps.

- This collaborative governmentwide strategy involves partnering with the Office of Management and Budget and the Office of Science and Technology in the Executive Office of the President as well as interagency councils and the Federal agencies.
- Currently, we are mapping the existing Federal cybersecurity workforce using OPM's new Cybersecurity Data Element Standard that recognizes the value of the NICE Framework.
- Our goal is that this new dataset in fiscal year 2015 and beyond will be a driving force that aids Federal agencies in getting the workforce they need.
- The re-categorizing of Federal positions with cybersecurity work will tell us what skills are in demand and what skills need to be refreshed or developed.
- Our job announcements will be designed to get the candidate quality desired by our hiring managers.
- Our training and development opportunities will be better designed to attract and retain the workforce we need.

*Question.* One theme you mentioned in your testimony was related to OPM's legacy IT system. How much of the OPM budget goes to Demonstration, Modernization, and Enhancement of IT systems as opposed to supporting existing and ongoing programs and infrastructure? How has this changed in the last 5 years?

Answer. OPM's annual IT Spend from fiscal year 2012 to fiscal year 2016 for Development, Modernization and Maintenance (DME) and Operations and Maintenance (O&M) as reported to OMB is outlined below.

- Fiscal Year 2012: DME: \$63,724,442; O&M: \$201,539,995;  
Total: \$265,264,437;
- Fiscal Year 2013: DME: \$97,273,199; O&M: \$211,815,787;  
Total: \$309,088,986;
- Fiscal Year 2014: DME: \$69,299,462; O&M: \$281,880,002;  
Total: \$351,179,464;
- Fiscal Year 2015: DME: \$110,724,682; O&M: \$257,968,435;  
Total: \$368,693,117;
- Fiscal Year 2016: DME: \$61,670,770; O&M: \$310,075,505;  
Total: \$371,746,275

*Question.* What are the 10 highest priority IT investment projects that are under development in your agency? Of these, which ones are being developed using an "agile" or incremental approach, such as delivering working functionality in smaller increments and completing initial deployment to end-users in short, 6-month timeframes? Please describe how the OPM IT plan developed in your first 100 days at the agency reflects this encouraged development method.

Answer. The table below shows the high priority IT projects that are currently under development at OPM. The IT Strategic Plan has served as a catalyst for the Investment Teams to make the transition to Agile and/or incremental development a top priority. Ultimately, moving development from a waterfall to agile methodology allows for more efficient and effective project management and is paramount to the long-term success of projects at OPM.

| #  | Project                                                                                                           | Investment                                  | Using Agile Development?                                                                                              |
|----|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 1  | USAJOBS .....                                                                                                     | USAJOBS .....                               | Yes                                                                                                                   |
| 2  | Enterprise Case Management System (ECMS).                                                                         | ECMS .....                                  | Yes, it is a contract requirement for the implementation of the software which is currently in the acquisition stage. |
| 3  | Shell—Infrastructure Improvement Project.                                                                         | Enterprise Infrastructure Operations (EIO). | Yes, the migration of existing applications to Shell will be done using an agile methodology.                         |
| 4  | Legacy Migration .....                                                                                            | EPIC Transformation .....                   | No. Project is on hold.                                                                                               |
| 5  | Electronic Official Personnel Folder (eOPF).                                                                      | eOPF .....                                  | Yes                                                                                                                   |
| 6  | EHRI Data Warehouse .....                                                                                         | EHRI Data Warehouse .....                   | Yes                                                                                                                   |
| 7  | Retirement Data Repository .....                                                                                  | eOPF .....                                  | Yes                                                                                                                   |
| 8  | New USA Staffing .....                                                                                            | USA Staffing System .....                   | Yes                                                                                                                   |
| 9  | Legacy USA Staffing to include core USA Staffing, Application Manager, On Boarding Manager and Selection Manager. | USA Staffing System .....                   | Yes                                                                                                                   |
| 10 | USA Performance .....                                                                                             | USA Performance .....                       | Yes                                                                                                                   |

*Question.* To ensure that steady State investments continue to meet agency needs, OMB has a longstanding policy for agencies to annually review, evaluate, and report on their legacy IT infrastructure through Operational Assessments. What Operational Assessments have you conducted and what were the results?

*Answer.* As per OMB's requirement, the major investments listed below are in the O&M stage and have conducted an Operational Analysis (OA) or Post-Implementation Review (PIR). All of the OAs and PIRs touch on number issues and are many pages long (10+). Hence forth, it is difficult to summarize in a few sentences as to whether all aspects of the investment are performing well.

- USAJOBS
- USA Staffing System
- Enterprise Infrastructure Operations (EIO)
- EHRI electronic Official Personnel Folder (eOPF)
- EHRI Data Warehouse
- Consolidated Business Information System (CBIS)

*Question.* What are the 10 oldest IT systems or infrastructures maintained by the Office of Personnel management? How old are they? Would it be cost-effective to replace them with newer IT investments?

*Answer.* The applications that are the oldest are in OPM's Retirement Services and Federal Investigative Services. Retirement Services has more than 60 applications dating back to the mid-1980's. OPM's modernization plan is replacing these applications with newer IT. Our goal is to move into a more modern infrastructure environment and to move off of the main frame.

*Question.* How does OPM's IT governance process allow for your agency to terminate or "off ramp" IT investments that are critically over budget, over schedule, or failing to meet performance goals? Similarly, how does your agency's IT governance process allow for your department/agency to replace or "on-ramp" new solutions after terminating a failing IT investment?

*Answer.* OPM established an Investment Review Board (IRB) as the authoritative body to review and recommend investment priorities to the OPM Director for IT spending. The current IRB charter States that one of the IRB functions is to: "Monitor ongoing information technology investments against their projected costs, schedules, and benefits, and take action to recommend continuation, modification, or termination." The IRB is comprised of senior management of all OPM offices which meet on a quarterly or as-needed basis to receive IT Investment assessment briefings. If a new solution or replacement is required, the IRB would receive a Business Case from the IT Investment. The IRB would review and provide disapproval or approval of the Business Case.

*Question.* What IT projects has your agency decommissioned in the last year? What are your agency's plans to decommission legacy IT projects this year?

*Answer.* OPM has not decommissioned any IT projects in the last year. However, OPM has initiated multiple IT projects to replace numerous legacy IT projects. These include the Shell project which will incorporate numerous technology upgrades to the OPM IT infrastructure; and the Enterprise Case Management System (ECMS) project which will replace legacy case management systems.

*Question.* The newly-enacted Federal Information Technology and Acquisition Reform Act of 2014 (FITARA, Public Law 113–291) directs CIOs to conduct annual reviews of their department’s IT portfolio. While OPM is not subject to FITARA, does OPM conduct these types of IT portfolio reviews? If so, please describe your agency’s efforts to identify and reduce wasteful, low-value or duplicative information technology (IT) investments as part of these portfolio reviews.

*Answer.* OPM is subject to FITARA and agrees with its efforts to centralize the oversight process for IT investments. The required elements of FITARA will position OPM to address previous issued IG findings and recommendations. OPM believes this shift will greatly strengthen its efforts to ensure effective and efficient spending on IT investments.

Through improved governance and oversight of IT investments and initiative development, OPM is reducing the redundancy of systems and capabilities across the enterprise. For example, an enterprise case management system has been put into place, which will remove duplication and assist in fulfilling mission critical needs for FIS and Retirement Services.

*Question.* In 2011, the Office of Management and Budget (OMB) issued a “Cloud First” policy that required agency Chief Information Officers to implement a cloud-based service whenever there was a secure, reliable, and cost-effective option. How many of the agency’s IT investments are cloud-based services (Infrastructure as a Service, Platform as a Service, Software as a Service, etc.)? What percentage of the agency’s overall IT investments are cloud-based services? How has this changed since 2011?

*Answer.* OPM’s new infrastructure is essentially a cloud based service. It will be infrastructure as a service to our program offices, including software, storage, and security as a service. We are moving to a total cloud based methodology. As OPM in its modernization plan is collapsing the five data centers that it currently operates into two commercial data centers, we are building our cloud service as a high security center.

*Question.* Provide short summaries of three recent IT program successes—projects that were delivered on time, within budget, and delivered the promised functionality and benefits to the end user. How does your agency define “success” in IT program management? What “best practices” have emerged and been adopted from these recent IT program successes? What have proven to be the most significant barriers encountered to more common or frequent IT program successes?

*Answer.* USAJOBS utilizes modern user-centered design practices, agile software development, data analytics, and DevOps to deliver high-value features and enhancements every 9–12 weeks. Leveraging human-centered design methodology, USAJOBS engages users early and often in the design process to ensure that features are designed and developed to provide the best possible user experience. USAJOBS employs Agile software development practices to rapidly adjust to changing customer priorities, allowing the program office to always be working on the top user priority and deliver completed software features after every three week sprint.

USAJOBS creates a measurement plan for all new features, defining measurable goals that can be captured in real-time. Gone are spreadsheets, static PowerPoints, and manual performance monitoring—USAJOBS monitors all key performance indicators via a real-time analytics dashboard that is populated by our data warehouse. Since 2013 USAJOBS has taken methodical steps to increase the efficiency of our development pipeline by employing DevOps best practices. Practices like continuous integration, automated testing, and automated security scanning have decreased the technical overhead surrounding software deployments and increased our security posture. These best practices have increased customer satisfaction, changed user behaviors and reduced support costs while gaining efficiencies in delivering value to the customer. The following three IT programs are examples of how OPM has successfully applied IT best practices to deliver systems that reflect Federal agencies business needs and priorities:

- USA Staffing* is OPM’s Talent Acquisition System for Federal agencies. Created by OPM and informed by the experience of more than 50 agencies, USA Staffing helps agencies acquire, assess, certify, select, and onboard qualified candidates in alignment with Merit System Principles and Veterans Preference. USA Staffing is tightly integrated with USAJOBS and compliant with Federal hiring regulations and Federal Information Technology (IT) requirements. Through Agile IT, USA Staffing and USAJOBS share technical solutions, such as user authentication and document upload processes, and collaborate to carry out joint research on governmentwide priorities, including encryption solutions.
- OPM’s *HR Solutions* (HRS) and Chief Information Officer (CIO) completed a multi-year project (launched in September 2012) to upgrade USA Staffing. OPM initiated the Upgrade to: (1) ensure modern technologies are in place to support

capacity demands; (2) improve speed to mission by enabling USA Staffing to be more responsive to customer requirements and OPM initiatives; and (3) expand data analytics that can be used by management to improve the hiring process. Of note, USA Staffing accounted for 78 percent of Federal job postings on USAJOBS in fiscal year 2014.

Barriers to success include the lengthy hiring process which often delays necessary hires, and the Federal contracting process which inhibits the Agile System Development Life Cycle.

—*USA Performance* (USAP) was developed in direct response to the overwhelming need across Government for an automated performance management tool. USAP addresses a critical gap in available technology to appropriately automate this fundamental human resources function in all Federal agencies. USAP uses the latest IT development principles (Agile) and technology to build a cost-effective and desirable system. These principles include focusing on the most valuable functionality with constant stakeholder input and engaging in frequent planning to ensure successful software delivery. USAP operates in 4 week sprints to develop and test new functionality. As such, the system (initially released in July 2014) was developed on schedule (less than 16 months) and under budget estimates. Since the initial release, USAP has had six subsequent releases to enhance functionality. In the first 6 months of planning, USAP convened key representatives from 10 Federal agencies to capture requirements for designing USAP and gain better understanding of their business needs. USAP also facilitates frequent usability testing with potential end users from a variety of agencies on system features as the features are being developed. This results in faster approval, increased satisfaction, and easier adoption by pilot agencies. Through continuous stakeholder involvement, the development team and the programmers can focus on developing the highest value functions in the tool. OPM continues to facilitate monthly advisory board meetings for agencies to provide input and feedback on USAP enhancements and other changes now that agencies are using the tool. USAP is an evolving, growing system. As a result of these development principles, USAP anticipates continued program success. USAP has been acknowledged outside of OPM for its innovation and efforts to revolutionize performance management. In 2014, USAP won the Nextgov Bold Award, the People's Choice Award, and received third place from HCMG for "Best Implementation of an Enterprise Technology System."

#### QUESTIONS SUBMITTED BY SENATOR CHRISTOPHER A. COONS

*Question.* Do you know exactly what your requirements are for the IT modernization project so that the contractor is not in the driver's seat to determine your requirements for you (which has led other agencies' IT projects to their downfall)?

*Answer.* Yes. OPM's Federal employees created the requirements for Shell and the phased approach that would be used to implement the plan before hiring contractor assistance with execution of the plan.

*Question.* Have you reviewed other agencies' successful IT projects to use as a model?

*Answer.* Yes. OPM consulted with other Federal agencies to hear of lessons learned and leading practices prior to full development of requirements, scope and budget.

*Question.* GAO has recommended that for IT projects to be successful, they should be broken down into smaller segments, which allows for better oversight of the project, increasing odds of avoiding schedule delays and cost overruns. Do you feel that this project is designed in that manner or are there improvements that can be made in that regard?

*Answer.* Yes. OPM's IT Modernization Plan was broken down into 4 phases to better manage requirements, budgets and execution. The four phases are:

- Phase 1—Tactical: Deployment of expanded security tools to strengthen existing OPM network.
- Phase 2—Shell: Design and deploy new data center infrastructure.
- Phase 3—Migration: Re-architect OPM applications to make best use of Shell and current technologies and to find efficiencies across applications through reuse.
- Phase 4—Decommission: Remove hardware from existing network as applications move to Shell.

*Question.* Has the Chief Information Officer had experience handling projects of this dimension?

Answer. Yes. Mrs. Seymour served as the Executive Director, Enterprise Human Resource Information Systems where she was responsible for providing Department of Defense wide information technology solutions to meet the needs of 35,000 HR specialists, DOD civilian employees, and military and civilian managers and leaders. She began her Federal career in 1978 and has concentrated primarily in the area of information technology, especially its ability to transform the workforce and business of the Federal Government, acquisition, financial management, and human resources management.

*Question.* Do you expect this project to be on OMB's IT Dashboard?

Answer. Yes, the 10 highest priority projects currently are or are expected to be on OMB's IT Dashboard.

#### CONCLUSION OF HEARINGS

Senator BOOZMAN. With that, the subcommittee hearing is adjourned.

[Whereupon, at 12:44 p.m., Tuesday, June 23, the hearings were concluded, and the subcommittee was recessed, to reconvene subject to the call of the Chair.]