OPM: DATA BREACH

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 16, 2015

Serial No. 114–60

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

99–659 PDF WASHINGTON : 2016

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

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

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

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
TROY D. STOCK, *IT Subcommittee Staff director*
JENNIFER HEMINGWAY, *Government Operations Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*

CONTENTS

OPM: DATA BREACH

Tuesday, June 16, 2015

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

The committee met, pursuant to call, at 10:11 a.m., in Room 2247, Rayburn House Office Building, the Honorable Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Jordan, Walberg, Amash, Gosar, Massie, Meadows, DeSantis, Mulvaney, Walker, Hice, Russell, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Norton, Lynch, Connolly, Cartwright, Kelly, Lawrence, Lieu, Watson Coleman, Plaskett, DeSaulnier, Boyle, Welch, and Lujan Grisham.

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

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

Mr. Cummings will be with us momentarily. Another committee assignment is also pressing on his schedule.

Last week we learned that the United States of America may have had what may be the most devastating cyber attack in our Nation's history, and that this may have been happening over a long period of time.

As we sit here this morning, there is a lot of confusion about exactly what personal information for millions of current and former Federal employees and workers were exposed through the latest data breach at the Office of Personnel Management.

OPM initially reported that the personal information of more than 4 million Federal employees was exposed during this attack. More recent public reports suggest that the breach was perhaps much worse than that.

It is also unclear exactly what information was exposed. We would like to know what information was exposed, over what period of time, and who has this vulnerability.

It would also be great to know who had conducted this attack. And I think we need to have candor with not only the Federal employees, but the American people as well.

The breach potentially included highly sensitive personal background information collected through the security clearance applications. We would like clarity on that position as well.

The loss of this information puts our Federal workforce at risk, particularly our intelligence officers and others working on sensitive projects throughout the globe. But we are concerned about

each and every Federal worker and the public who has interacted with the Government and entrusted this information with the Government. We need to understand why the Federal Government, and OPM in particular, is struggling to guard some of our Nation's most important information.

The fact that OPM was breached should come as no surprise giving its troubled track record on data security. This has been going on for years and it is inexcusable.

Each year, the Office of Inspector General reviews and rates its respective agency's compliance with the Federal Information Security standards. According to the last eight years of IG reports, OPM's data security posture was akin to leaving all the doors and windows open in your house and expecting that nobody would walk in and nobody would take any information. How wrong they were.

Since 2007, the OPM Inspector General rated OPM's data security as a "material weakness" because the agency had no IT policies or procedures that can come anywhere close to something that could be used as an excuse for securing the information.

It is unbelievable to think the agency charged with maintaining and protecting all personal information of almost all former and current Federal employees would have so few information technology policies or procedures in place.

Let me just kind of read through some of the reports that have happened through the course of the years.

This is the inspector general from fiscal year 2009: This year we are expanding the material weakness to include the agency's overall information security governance programs and incorporating our concerns about the agency's information security management structure. The continuing weakness at OPM's information security program result directly from inadequate governance. Most, if not all, of the exceptions we noted this year resulted from a lack of necessary leadership, policy, and guidance.

Go to fiscal year 2010: We continue to consider the IT security management structure insufficient staff and the lack of policies and procedures to be a material weakness in OPM's IT security program.

Fiscal year 2011: We continue to believe that the information security governance represents a material weakness at OPM's IT security program.

Fiscal year 2012: Throughout fiscal year 2012, the OCIO, the Office of the Chief Information Officer, continued to operate with a decentralized IT security structure that did not have the authority or resources available to adequately implement new policies. However, the material weakness remains open in this report as the agency's IT security function remained decentralized throughout fiscal year 2012, FISMA reporting period, and because of the continued instances of non-compliance with FISMA requirements.

It goes on later: The OCIO's response to our draft audit report indicated that they disagree with the classification of the material weakness because of the program that OPM has made with its IT security program and because there was no loss of sensitive data during the fiscal year. But as the inspector general pointed out, however, the OCIO's statement is inaccurate, as there were in fact numerous information security incidents in fiscal year 2012 that

led to the loss or unauthorized release of mission-critical and sensitive data.

They couldn't even decide and agree that they had lost the data back in fiscal year 2012, let alone actually solve the problem.

Go to fiscal year 2013. Again, the inspector general: The findings of this audit report highlight the fact that OPM's decentralized governance structure continues to result in many instances of noncompliance with FISMA requirements; therefore, we are again reporting this issue as a material weakness in fiscal year 2013.

Fast forward to fiscal year 2014. This is November of 2014: Eleven major OPM information systems are operating without valid authorization. This represents a material weakness in the internal control structure at OPM's IT security program.

It goes on: OPM does not maintain a comprehensive inventory of servers, databases, and network devices. They didn't even know what they have. They don't even know what is in the inventory.

Program offices are not adequately incorporating known weakness into plans of action and milestones, and the majority of systems are 120 days overdue. OPM continues to implement its continuous monitoring plan; however, security controls for all OPM systems are not adequately tested in accordance with their own policies. Not all OPM systems have conducted contingency plan tests in fiscal year 2014. Several information security agreements between OPM and contract operated information systems have expired. Multi-factor authentication is not required to access OPM systems in accordance with the OMB memorandum.

This has been going on for a long time. And yet, when I read the testimony that was provided here, we are about to hear some say, hey, we are doing a great job. You are not. It is failing.

This went on for years and it did not change. The inspector general found that 11 of the 47 major information systems, or roughly 23 percent, at OPM lacked proper security authorization, meaning the security of 11 major systems was completely outdated and unknown. Five of the 11 systems were in the Office of the Chief Information Officer, Ms. Seymour. They are in your office, which is a horrible example to be setting as the person in charge of the agency's data security.

The IG only recently upgraded OPM to a "significant deficiency." In November 2014, FISMA, over 65 percent of all systems operated by OPM reside on two of the systems without valid authorization. Sitting on two systems, no valid authorization, 65 percent of the information.

For any agency to consciously disregard its data security for so long is grossly negligent. And the fact that the agency that did this is responsible for maintaining highly sensitive information for almost all Federal employees, in my opinion, is even more egregious.

OPM isn't alone. A number of other agencies also suffered breaches in the last year. This later cyber hack comes on the heels of several data breaches across the Government, including the Postal Service, the State Department, the Internal Revenue Service, the Nuclear Regulatory Commission, and even the White House.

At the same time, government is spending more and more on information technology. Last year, across government, we, the Amer-

ican people, spent almost $80 billion on information technology, and it stinks. It doesn't work, $80 billion dollars later. And the person in charge of security, the person who is in charge of making sure there is authentication of our systems, even in her own office there isn't the authorization needed.

OPM is not alone in the blame for this failure. The Office of Management and Budget has the responsibility for setting standards for Federal cybersecurity practices, and it is OMB's job to hold agencies accountable for complying and enforcing these standards.

The Department of Homeland Security has been given the lead responsibility for serving as the Federal Government's so-called geek squad to monitor day-to-day cybersecurity practices, but the technical tools that DHS has deployed to try to protect Federal networks apparently isn't doing the job.

While DHS has developed EINSTEIN to monitor Government networks, it only detects known intruders, proving that it is completely useless in the latest OPM hacks.

The status quo cannot continue. We have to do better. We are talking about the most vital information of the most sensitive nature of the people that we care about most. The people entrust that information to OPM, and through the years it has been a complete and total utter failure, to the point we find ourselves where millions of Americans are left wondering what somebody knows about them. What are they supposed to do?

And I have read the letter that you have been sending out to employees, and it is grossly inadequate. It is grossly inadequate, and that is why we are having this hearing today.

We do appreciate you all being here.

I think what we are going to do now is I would like to recognize the gentleman from Texas who is the chairman of the subcommittee that we have on IT. We at the Oversight and Government Reform Committee have set up a new subcommittee that deals just with IT issues.

We are honored and pleased to have Mr. Hurd chairing that committee, so I will now recognize the gentleman from Texas, Mr. Hurd, for five minutes.

Mr. HURD. Thank you, Mr. Chairman.

Not only as the head of the subcommittee, but as a former intelligence officer who has been through background investigation and whose information probably resides with OPM, I am concerned.

Today's hearing is just another example of the undeniable fact that America is under constant attack. It is not bombs dropping or missiles launching; it is the constant stream of cyber weapons aimed at our data. From private sector innovations to military seekers, our enemies are attempting to rob this Country on a daily basis, and, unfortunately, they are succeeding.

The worst of these cyber attacks are not coming from the caves of Afghanistan or Syria, but from air conditioned office buildings in China, Iran, and Russian, far from battlefields. These hackers work with impunity, knowing that their actions have no consequences.

This is not only a question of how we can protect our networks and data, but of how we define the appropriate responses for digital and digital attacks. This is one of the questions I have been

asking for years and I have continued to ask in my role as chairman of the Information Technology Subcommittee.

It is no secret that Federal agencies need to improve their cybersecurity posture. We have years and years of reports highlighting the vulnerabilities of Federal agencies from legacy systems to poor FISMA compliance. And while there have been improvements, they have not kept pace with the nature of the threats we are facing.

But until agency leadership takes control of these basic cybersecurity measures, things like strong authentication, network monitoring, encrypting data, and segmentation, we will always be playing catch-up against our highly sophisticated and well-resourced adversaries.

I welcome the witnesses here today and look forward to their testimony.

Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the gentlewoman from Illinois, the ranking member of the subcommittee on IT, Ms. Kelly, for five minutes.

Ms. KELLY. Thank you, Mr. Chair.

I want to thank our expert witnesses for their participation today, and I thank the chairman and ranking member for holding this important hearing on the OPM data breach.

As you know, I have the privilege of serving as the ranking member of the IT subcommittee. The issue of data breach is something that Chairman Hurd and I are quite concerned with, and we are looking forward to working with our colleagues to be active in addressing this issue.

All of us here today should be quite concerned. The OPM breach has raised significant questions about how adequately the personnel information of government employees is stored on government networks. We know that every day our government and American businesses face a barrage of cyber threats.

We are reminded of many of the high-profiled breaches on some of our Nation's most important companies, but there are everyday cyber intrusions of our data that aren't making the headlines. Whether it is criminals beyond our borders profiting from fraud and identity theft, domestic competitors who steal intellectual property to gain advantage, or hacktivists looking to make a statement against governments, cyber crime threatens our national security and economic prosperity.

Data breaches probably won't end any time soon, but they are something that we can be more aggressive in addressing. As we catch on to cyber attackers' methods, these bad actors will look to innovate their way around newly integrated cyber defenses. This is why we must be just as innovative. That is why we must have a frank conversation today and prepare a multi-front strategy to ward off and diminish the possibility of future data breaches.

So I thank the committee and our witnesses again for this opportunity to examine the OPM attack and, with that, I yield back.

Chairman CHAFFETZ. I thank the gentlewoman.

It is our intention to hear the ranking member's, Mr. Cummings, statement, but I think what we will do now is swear in the witnesses, hear their statements, then we will go to Mr. Cummings before we get to questions, if that is okay with everybody.

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

We will now recognize our first panel of witnesses.

We are pleased to welcome the Honorable Katherine Archuleta, who is the Director of Office of Personnel Management; Dr. Andy Ozment, Assistant Secretary of the Office of Cybersecurity and Communications at the National Program Preparedness Directorate at the United States Department of Homeland Security; Mr. Tony Scott, U.S. Chief Information Officer of the Office of E–Government and Information Technology at the U.S. Office of Management and Budget; Ms. Sylvia Burns, Chief Information Officer of the United States Department of Interior; Ms. Donna Seymour, Chief Information Officer of the United States Office of Personnel Management; and Mr. Michael Esser, Assistant Inspector General for Audits, Office of The Inspector General at the United States Office of Personnel Management.

We welcome you all.

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

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

[Witnesses respond in the affirmative.]

Chairman CHAFFETZ. Thank you. Please be seated.

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

In order to allow time for discussion, we would appreciate your limiting your testimony to five minutes. Again, please limit your comments to five minutes. I will be a little bit generous, but five minutes, if you could, and then your entire written statement will be entered into the record.

At the conclusion of those, then we will hear from Mr. Cummings with his opening statement and we will go to questions from there.

So, with that, we will now recognize Ms. Archuleta, the Director of the Office of Personnel Management, and you are now recognized for five minutes.

WITNESS STATEMENTS

STATEMENT OF THE HONORABLE KATHERINE ARCHULETA

Ms. ARCHULETA. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, I am here today to talk to you about two successful intrusions into OPM's systems and data. But first I want to deliver a message to Federal employees, retirees, and their families. The security of their personnel data is of paramount importance. We are committed to full and complete investigation of these incidents and are taking actions to mitigate vulnerabilities exposed by their intrusions.

When I was sworn in as Director 18 months ago, I recognized that in order to build and manage an engaged, inclusive and well-trained workforce, that we would need a thorough assessment of the state of information technology at OPM. I immediately became aware of vulnerabilities in our aging legacy systems and I made

the modernization and the security of our network one of my top priorities.

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. These attacks will not stop. If anything, they will increase.

Within the last year, we have undertaken an aggressive effort to update our cybersecurity posture, adding numerous tools and capabilities to our networks. As a result, in April of 2015, an intrusion that predated the adoption of these security controls was detected. We immediately contacted the Department of Homeland Security and the FBI, and together with these partners, initiated an investigation to determine the scope and the impact of the intrusion. In May, the interagency incident response team concluded that the exposure of personnel records had occurred, and notifications to affected individuals began on June 8th and will continue through June 19th.

As part of our ongoing notification process, we are continuing to learn more about the systems that contributed to individuals' data potentially being compromised. These individuals were included in the previously identified population of approximately 4 million individuals and are being appropriately notified. 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.

During the course of the ongoing investigation, the interagency incident response team concluded later in May that additional systems were likely compromised. This separate incident, which also predated deployment of our new security tools and capabilities, remains under investigation by OPM and our interagency partners.

However, there is a high degree of confidence that 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 exfiltrated. While we have not yet determined its scope or its impact, we are committed to notifying those individuals whose information may have been compromised as soon as practicable.

Throughout these investigations, we have provided regular updates to congressional leadership and the relevant committees of these incidents. But for the fact that we implemented new, more stringent security tools, we would have never known that malicious activity had previously existed on that 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 and working with our partners at DHS, we have immediately implemented additional security measures to protect sensitive information and to take steps toward building a simplified, modern, and flexible network structure. We continue to execute on our aggressive plan to modernize OPM's platform and bolster security tools.

Our 2016 budget request includes an additional $21 million above 2015 funding levels to further the support of 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 our cyber posture, including advanced tools such as database encryption, stronger firewalls, storage devices, and masking software. The funding will also support the redesign of OPM's legacy network.

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

[Prepared statement of Ms. Archuleta follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF
THE HONORABLE
KATHERINE ARCHULETA
DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"OPM: Data Breach"

June 16, 2015

Chairman Chaffetz, Ranking Member Cummings and Members of the committee:

When I was sworn in as the Director of the U.S. Office of Personnel Management (OPM) 18 months ago, I recognized that in order to meet our goals to build and manage an engaged, inclusive, and well-trained workforce that we would need a thorough assessment of the state of information technology (IT) at OPM. When I was sworn in I said that I would develop an IT strategic plan in my first 100 days and delivered on that promise in February 2014. 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 *Strategic IT Plan*, is to innovate IT infrastructure at OPM in a way that leverages cybersecurity best practices and protects the sensitive information entrusted to the agency.

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. In an average month, OPM, for example thwarts 10 million confirmed intrusion attempts targeting our network. These attacks will not stop – if anything, they will increase. I'm here today to talk to you

about two successful intrusions that were detected recently but took place in the past. I'm also here to deliver a message to Federal employees, retirees, and their families: the security of your personal data is of paramount importance. We are committed to a full and complete investigation of these incidents and are taking action to mitigate vulnerabilities exposed by intrusions.

Strengthening and Enhancing OPM's Cybersecurity

As I stated earlier, within the last year, OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. We are focused on protecting our legacy network to the maximum extent possible as we design a more modern system. As part of these efforts, we have improved network monitoring and logging capability to contain intrusions and ensure data is protected. Additional firewalls were installed in the network to better segment systems and data, and enhanced authentication for remote access is being enforced.

As a result of our 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. 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 intrusion as the intrusion affecting personnel records.

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 – remains under investigation by OPM and our interagency partners. 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. OPM and its interagency partners have briefed the House Permanent Select Committee on Intelligence on their preliminary findings and FBI Director Comey briefed the Senate Select Committee on Intelligence. 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 the Department of Homeland Security (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. OPM's 2016 budget request includes 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 FY2014 and FY2015 to improve OPM's cyberposture, including advanced tools such as database encryption, stronger firewalls and storage devices, and masking software. The funding will also support the redesign of OPM's legacy network.

Conclusion

In conclusion, I want to emphasize that cyber security issues that the Government is facing is a problem that has been decades in the making, due to a lack of investment in federal IT systems and a lack of efforts in both the public and private sectors to secure our internet infrastructure. We discovered these intrusions because of our increased efforts in the last eighteen month 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.

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

Chairman CHAFFETZ. Thank you.
Dr. Ozment.

STATEMENT OF ANDY OZMENT

Mr. OZMENT. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, I appreciate the opportunity to appear before you today.

Like you, my fellow panelists, and countless Americans, I am deeply concerned about the recent compromise at OPM. I am personally dedicated to ensuring that we take all necessary steps to protect our Federal workforce and to drive forward the cybersecurity of the entire Federal Government.

Director Archuleta and my written statement both spoke to the facts of the OPM incident, so I want to focus my remarks on how DHS is accelerating our efforts to protect the Federal Government.

This morning I will discuss how the Department of Homeland Security is protecting civilians, Federal agencies, and helping those agencies better protect themselves.

Under legislation passed by this Congress last year, Federal agencies are responsible for their own cybersecurity. However, DHS provides a common baseline of security across the civilian government and helps agencies better manage their cyber risks through four key efforts. First, we protect agencies by providing a common set of capabilities through the EINSTEIN and Continuous Diagnostics and Mitigation, or CDM, programs. Second, we measure and motivate agencies to implement best practices; third, we serve as a hub for information sharing. Finally, we provide incident response assistance when agencies suffer a cyber intrusion.

I will focus this morning on the first area, how DHS provides a baseline of security across the Federal Government through EINSTEIN and CDM. I have described the other three areas in my written statement and am happy to take your questions on them.

Our first line of defense against cyber threats is the EINSTEIN system, which protects agencies at the perimeter. A useful analogy is that of a physical government facility. In this analogy with the physical world, EINSTEIN 1 is similar to a camera at the entrance to the facility that records the traffic coming and going, and identifies anomalies in the number of cars.

EINSTEIN 2 adds the ability to detect suspicious cars based upon a watch list and to alert security personnel when a prohibited vehicle is identified. EINSTEIN 2 does not stop cars, but it does set off an alarm.

EINSTEIN 1 and 2 are fully deployed in screening approximately 90 percent of all Federal civilian traffic, all of the traffic that goes through trusted Internet connections.

The latest phase of the program, known as EINSTEIN 3A, is akin to a guard post at the highway that leads to multiple government facilities. EINSTEIN 3A uses classified information to look at the cars and compare them with a classified watch list. It then actively blocks prohibited cars from entering the facility.

We are accelerating our efforts to protect all civilian agencies with EINSTEIN 3A. The system now covers 15 Federal civilian agencies, with over 930,000 Federal personnel, which is approximately 45 percent of the civilian government, and those are pro-

tected with at least one of two security countermeasures. That is about double the coverage we had just nine months ago.

During this time, EINSTEIN 3A has blocked over 550,000 attempts to access potentially malicious Web sites, which is one of our two countermeasures. EINSTEIN played a key role in identifying the recent compromise of OPM data at the Department of Interior.

As we accelerate EINSTEIN deployment, we also recognize that security cannot be achieved through only one type of tool. EINSTEIN will never be able to block every threat. For example, it must be complemented with systems and tools to monitor inside agency networks. Our CDM program addresses this challenge.

Returning to our analogy of a government facility, CDM Phase 1 allows agencies to continuously check building locks and security cameras to ensure they are operated as intended. Continuing the analogy, the next two phases will monitor personnel in the facility to ensure they are not engaged in unauthorized activity, and it will assess activity across the facility to detect unusual patterns.

We have provided CDM Phase 1 capabilities to eight agencies, covering over 50 percent of the Federal Government, and we expect to cover 97 percent of the Government by the end of this fiscal year.

Now, the deadlines I have just told you are when DHS will provide a given capability. It will take a few additional months for agencies to fully implement their side of both EINSTEIN and CDM once they are available. And, of course, agencies must supplement EINSTEIN and CDM with additional tools appropriate to their needs.

I would like to conclude by noting that Federal agencies are a rich target and will continue to experience frequent attempted intrusions. This problem is not unique to the government. As our detection methods continue to improve, we will in fact detect more incidents, incidents that are already occurring and we just didn't know it yet.

The recent breach of OPM is emblematic of this trend, as OPM was able to detect the intrusion by implementing cybersecurity best practices recommended by DHS. We are facing a major challenge in protecting our most sensitive information against sophisticated, well resourced, and persistent adversaries.

Further, the entire Nation is now making up for 20 years of under-investment in our Nation's cybersecurity in both the public and private sectors. In response, we in the government are accelerating the deployment of the tools we have and are bringing cutting-edge capabilities online, and we are asking our partner agencies and Congress to take action and work with us to strengthen the cybersecurity of Federal agencies.

Thank you again for the opportunity to appear today, and I look forward to any questions.

[Prepared statement of Mr. Ozment follows:]

Introduction

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, thank you for the opportunity to appear before you today. The Office of Personnel Management (OPM) compromise clearly demonstrates the challenge facing the Federal Government in protecting our citizens' and employees' personal information against sophisticated, agile, and persistent threats. Addressing these threats is a shared responsibility. I will discuss the Department's role in the recent compromise at OPM and how we are working with OPM and other agencies to accelerate improved cybersecurity across the Federal Government.

The Role of the Department of Homeland Security in Federal Cybersecurity

Cyber security, like physical security, requires layers of protections. The *Federal Information Security Modernization Act of 2014* specifies that federal agencies are responsible for their own cybersecurity. Although agencies must take the lead in their own cybersecurity, as OPM is currently doing, DHS helps federal agencies protect their systems using two programs: (1) EINSTEIN, a perimeter protection program that detects and blocks threats attempting to access agencies' unclassified networks, and (2) Continuous Diagnostics and Mitigation (CDM), a DHS program that provides federal civilian agencies with tools to monitor agencies' internal networks. In addition, DHS has the mission to provide a common baseline of security across the civilian government and help agencies manage their cyber risk. DHS assists agencies by measuring and motivating agencies to implement best practices, by serving as a hub for information sharing, and by providing incident response assistance when agencies suffer a cyber intrusion.

EINSTEIN

Like a fence around a physical building, EINSTEIN protects agencies' unclassified networks at the perimeter of each agency. Furthermore, EINSTEIN provides situational awareness across the government, as threats detected in one agency are shared with all others so they can take appropriate protective action. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

The first two versions of EINSTEIN – EINSTEIN 1 and 2 – identify abnormal network traffic patterns and detect known malicious traffic. This capability is fully deployed and screening all federal civilian traffic that is routed through a Trusted Internet Connection (a secure gateway between each agency's internal network and the Internet). EINSTEIN 3 Accelerated (EINSTEIN 3A), which actively blocks known malicious traffic, is currently being deployed through the primary Internet Service Providers serving the Federal Government. EINSTEIN 1 and 2 use only unclassified information, while EINSTEIN 3A uses classified information. Using classified indicators allows EINSTEIN 3A to detect and block many of the most significant cybersecurity threats. I am happy to discuss the Department's efforts to accelerate EINSTEIN 3A's deployment across the Federal civilian government, as well as the development of advanced malware and behavioral analysis capabilities that will automatically identify and separate suspicious traffic for further inspection, even if the precise indicator has not been seen before. We are examining best-in-class technologies from the private sector to evolve to this next stage of network defense. And as I will discuss later, EINSTEIN played a key role in understanding the recent compromise at OPM.

Continuous Diagnostics and Mitigation (CDM)

Security cannot be achieved through only one type of tool. EINSTEIN is a perimeter system, but it will never be able to block every threat. It must be complemented with systems and tools inside agency networks. Through the CDM program, DHS provides Federal civilian agencies with tools to monitor agencies' internal networks. I am happy to take any questions about how CDM protects networks and the role is play in cybersecurity, but first I want to address the current incident.

DHS's Role in the OPM Compromise

Leveraging the expertise and guidance provided by DHS, the Office of Personnel Management has spent the last year implementing improved cybersecurity capabilities across its networks. As a result, in April 2015, OPM became aware of a cybersecurity intrusion affecting one of its systems. As soon as OPM identified malicious activity on their network, they shared this information with the DHS National Cybersecurity and Communications Integration Center (NCCIC).

The NCCIC then used one of our programs – EINSTEIN 2, the intrusion detection and situational awareness tool – to look back in time for other compromises across the federal civilian government. Through this process, the NCCIC identified a potential compromise at another location with OPM data. Since the incident was identified, OPM has partnered with various federal agencies, including DHS and the Federal Bureau of Investigation (FBI), to go onsite to investigate and mitigate the intrusion. At the same time, OPM immediately implemented additional security measures and continues to improve the security of the information it manages.

In May 2015, during the investigation and in the process of applying mitigating controls provided by DHS, OPM identified evidence that personnel records for current and former federal employees had been compromised. This remains an active investigation, and DHS, the FBI, and other partners are working closely with OPM to determine the extent of the compromise and potential implications. Information regarding this incident may change as the investigation progresses.

One of the important roles DHS plays is helping share information across agencies, and in some cases, with the private sector. For example, as soon as OPM identified malicious activity on their network, they shared this information with DHS. DHS then developed a signature for the particular threat, and used EINSTEIN 2 to look back in time for other compromises across the federal civilian government. This same threat information is used by EINSTEIN 3A to block potential threats from impacting federal networks. Thus, DHS is using EINSTEIN 3A to ensure that this cyber threat could not exploit other agencies protected by the system. DHS is accelerating EINSTEIN 3A deployment across the Federal Government. While it is challenging to estimate the potential impact of a prevented event, each of these malicious DNS requests or emails that were blocked by EINSTEIN 3A may conceivably have led to a cybersecurity compromise of severe consequence.

DHS's Role in Federal Incident Reponses

Cybersecurity is about risk management, and we cannot eliminate all risk. Agencies that implement best practices and share information will increase the cost for adversaries and stop many threats. But ultimately, there exists no perfect cyber defense, and persistent adversaries will find ways to infiltrate networks in both government and the private sector. When an

incident does occur, the NCCIC offers on-site assistance to find the adversary, drive them out, and restore service. In Fiscal Year 2015, the NCCIC has already provided onsite incident response to 32 incidents -- nearly double the total in all of Fiscal Year 2014. The NCCIC also coordinates responses to significant incidents to give senior leaders a clear understanding of the situation and give operators the information they need to respond effectively. Similar to the recent incident at OPM, providing on-site incident response assistance also allows the NCCIC to identify indicators of compromise that can then be shared with other agencies and applied to EINSTEIN for broad protection across the Federal Government.

Cybersecurity Legislation

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced DHS's ability to work with the private sector and other federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. DHS is using the authority granted in one of those bills – the *Federal Information Security Modernization Act of 2014* – to direct Federal civilian Executive branch agencies to fix critical vulnerabilities on their Internet-facing devices through the recent issuance of a Binding Operational Directive.

Additional legislation is needed. I previously highlighted EINSTEIN's key role in identifying and mitigating an additional potential compromise during the OPM activity. The Department and Administration have a longstanding request of Congress to remove obstacles to the EINSTEIN program's deployment across federal civilian agency information systems by codifying the program's authorities and resolving lingering concerns among certain agencies. Some agencies have questioned how deployment of EINSTEIN under DHS authority relates to

their existing statutory restrictions on the use and disclosure of agency data. DHS and the Administration are seeking statutory changes to clarify this uncertainty and to ensure agencies understand that they can disclose their network traffic to DHS for narrowly tailored purposes to protect agency networks, while making clear that privacy protections for the data will remain in place. I look forward to working with Congress to further clarify DHS's authority to rapidly and efficiently deploy this protective technology.

In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be collated quickly in the NCCIC, analyzed, and shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

Conclusion

Federal agencies are a rich target and will continue to experience frequent attempted intrusions. This problem is not unique to the Federal Government – it is shared across a global cybersecurity community. The key to good cybersecurity is awareness and constant vigilance at machine speed. As our detection methods continue to improve, more events will come to light. The recent breach at OPM is emblematic of this trend, as OPM was able to detect the intrusion by implementing cybersecurity best practices recommended by DHS. As network defenders are

able to see and thwart more events, we will inevitably identify more malicious activity and disappoint the adversary's attempts to access sensitive information and systems. We are facing a major challenge in protecting our most sensitive information against sophisticated, well-resourced, and persistent adversaries. In response, we are accelerating deployment of the tools we have and are working to bring cutting-edge capabilities online. And we are asking our partner agencies and Congress to take action and work with us to strengthen the cybersecurity of Federal agencies.

Chairman CHAFFETZ. Thank you.

Mr. Scott, you have a very impressive background. Your joining the Federal Government is much appreciated. We look forward to hearing your testimony. You are now recognized for five minutes.

STATEMENT OF TONY SCOTT

Mr. SCOTT. Thank you, Chairman Chaffetz, Ranking Member Cummings, members of the committee. Thank you for the opportunity to appear before you today. And I appreciate the opportunity to speak with you about recent cyber incidents affecting Federal agencies.

I would like to start by highlighting a very important point, which has been mentioned already and of which I am sure you are aware. Both state and non-state actors who are well financed, highly motivated, and persistent are attempting to breach both government and non-government systems every day, and these attempts are not going away. They will continue to accelerate on two fronts, first, the attacks will become more sophisticated and, second, as we remediate and strengthen our own practices, our detection capabilities will improve. But that means we have to be as nimble, as aggressive, and as well-resourced as those who are trying to break into our systems.

Confronting cybersecurity threats on a continuous basis is our Nation's new reality, a reality that I faced in the private sector and am continuing to see here in my new role as Federal Chief Information Officer.

As Federal CIO, I lead the Office of Management and Budget's Office of E–Government and Information Technology. My office is responsible for developing and overseeing the implementation of Federal information technology policy. And even though my team has a variety of responsibilities, I will focus today's remarks on cybersecurity.

Under the Federal Information Security Modernization Act of 2014, most of us know this as FISMA, OMB is responsible for Federal information security oversight and policy issuance. OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security and the Department of Commerce National Institute of Standards and Technology.

As I mentioned in front of this committee in April, OMB also recently announced the creation of the first ever dedicated cybersecurity unit within my office. This is the team that is behind the work articulated in the fiscal year 2014 FISMA report which highlighted both the successes and challenges facing Federal agencies' cybersecurity programs.

In fiscal year 2015, the E–Gov Cyber Unit is targeting oversight through CyberStat reviews, prioritizing agencies with high risk factors as determined by cybersecurity performance and incident data. My colleagues will fully address the recent cyber incidents affecting the Office of Personnel Management, known as OPM.

In terms of the role of OMB, my office monitors very closely all reports of incidents affecting Federal networks and systems. We use these reports to look for trends and patterns, as well as for areas where our government-wide processes, policies, and practices

can be strengthened. We then update our guidance and coordinate with other agencies to ensure that that guidance is implemented.

As you heard from me last week, the recently-passed Federal Information Technology Acquisition Reform Act, known as FITARA, and our guidance associated with that legislation strengthens the role of the CIO in agency cybersecurity.

In this case, OPM notified OMB in April 2015 of an incident affecting data in transit in its network. OPM reported that they were working closely with various government agencies on a comprehensive investigation and response to this incident. We have been actively monitoring the situation and have engaged in making sure that there is a government-wide response to the events that OPM.

To further improve Federal cybersecurity infrastructure and to protect systems against these evolving threats, OMB launched a 30-day Cybersecurity Sprint last week. The Sprint will focus on two areas: first, an interagency team is creating a set of action plans and strategies to further address critical cybersecurity priorities; second, agencies were directed to accelerate efforts to deploy threat indicators, patch critical vulnerabilities, and tighten policies and practices for privileged users, and to dramatically accelerate implementation of multi-factor authentication.

In closing, I want to underscore a critical point I made at the beginning of this testimony: both State and non-State actors are attempting to breach government and non-government systems in a very aggressive way. It is not going to go away, and we are going to see more of it. Ensuring the security of information on Federal Government networks and systems will remain a core focus of the Administration as we move aggressively to implement innovative protections and response to new challenges as they arise. In addition to the actions we are taking, we also look forward to working with Congress on legislative actions that may further protect our Nation's critical networks and systems.

I thank the committee for holding this hearing and for your commitment to improving Federal cybersecurity. I would be pleased to answer any questions you may have.

[Prepared statement of Mr. Scott follows:]

Embargoed until Delivered

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF TONY SCOTT

UNITED STATES CHIEF INFORMATION OFFICER
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

June 16, 2015

Chairman Chaffetz, Ranking Member Cummings, members of the Committee, thank you for the opportunity to appear before you today. I appreciate the opportunity to speak with you about recent cyber incidents impacting Federal agencies.

I would like to start by highlighting a very important point of which you are probably already aware: both state and non-state actors who are well financed, highly motivated, are persistently attempting to breach both government and non-government systems. And these attempts are not going away. They will continue to accelerate on two dimensions: first, the attacks will continue to become more sophisticated, and secondly, as we remediate and strengthen our own practices, our detection capabilities will improve. That means that we have to be as nimble, as aggressive, and as well-resourced as those who are trying to break into our systems.

Confronting cybersecurity threats on a continuous basis is our nation's new reality– a reality that I faced in the private sector, and am continuing to see here in my new role as the Federal Chief Information Officer (CIO). As Federal CIO, I lead the Office of Management and Budget's (OMB) Office of E-Government & Information Technology (IT) (E-Gov). My office is responsible for developing and overseeing the implementation of Federal Information Technology policy. Even though my team has a variety of responsibilities, I will focus today's remarks on cybersecurity.

OMB's Role in Federal Cybersecurity

Under the Federal Information Security Modernization Act of 2014 (FISMA), OMB is responsible for federal information security oversight and policy issuance. OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security (DHS) and the Department of Commerce's National Institute of Standards and Technology (NIST).

As I mentioned in front of this committee in April, OMB also recently announced the creation of the first ever dedicated cybersecurity unit within the Office of E-Gov & IT: the E-Gov Cyber and National Security Unit (E-Gov Cyber). The creation of the E-Gov Cyber Unit reflects OMB's focus on conducting robust, data-driven oversight of agencies' cybersecurity programs,

monitoring and improving responses to major cyber security incidents, and issuing Federal guidance consistent with emerging technologies and risks.

This is the team behind the work articulated in the Fiscal Year (FY) 2014 FISMA report which highlighted both successes and challenges facing Federal agencies' cyber programs. In FY 2015, the E-Gov Cyber Unit is targeting oversight through CyberStat reviews, prioritizing agencies with high risk factors as determined by cybersecurity performance and incident data. Additionally, the Unit is driving FISMA implementation by providing agencies with the guidance they need in this dynamic environment. The top FY 2015 policy priority of the team is updating Circular A-130, which is the central government-wide policy document that establishes agency guidelines on how to manage information resources, to include best practices for how to secure those resources.

Recent Cyber Incidents Affecting the Office of Personnel Management (OPM)

My colleagues will fully address the recent cyber incidents affecting the Office of Personnel Management (OPM). In terms of the role of OMB, my office monitors very closely all reports of incidents affecting federal networks and systems. We use these reports to look for trends and patterns as well as for areas where our government-wide processes, policies, and other practices can be strengthened. We then update our guidance and then coordinate with other agencies to ensure that guidance is implemented. And as you heard from me last week, the recently passed Federal Information Technology Acquisition Reform Act (FITARA) and our guidance associated with the legislation strengthens the role of the CIO in agency cybersecurity

In this case, OPM notified OMB in April 2015 of an incident affecting data in transit in its network. OPM reported that they were working closely with various government agencies on a comprehensive investigation and response to this incident. We have been actively monitoring the situation and have been engaged in making sure that there is a government-wide response to the events at OPM.

Strengthening Federal Cyber Security Practices

To further improve Federal cyber infrastructure and protect systems against these evolving threats, last week OMB launched a 30-day Cybersecurity Sprint. The team is comprised of the Office of Management and Budget's (OMB) E-Gov Cyber and National Security Unit (E-Gov Cyber), the National Security Council Cybersecurity Directorate (NSC Cyber), the Department of Homeland Security (DHS), the Department of Defense (DOD), and other agencies. At the end of the review, the Government will create and operationalize a set of action plans and strategies to further address critical cybersecurity priorities and recommend a Federal Civilian Cybersecurity Strategy.

As part of the effort, OMB instructed Federal agencies to immediately take a number of steps to protect Federal information and assets and improve the resilience of Federal networks.

Specifically, Federal agencies must:

- Immediately deploy indicators provided by DHS regarding priority threat-actor techniques, tactics, and procedures to scan systems and check logs.
- Patch critical vulnerabilities without delay and report to OMB and DHS on progress and challenges within 30 days.
- Tighten policies and practices for privileged users.
- Dramatically accelerate implementation of multi-factor authentication, especially for privileged users.

Summary

In closing, I want to underscore a critical point I made at the beginning of this testimony: both state and non-state actors are attempting to breach both government and non-government systems. And this problem is not going to go away. It's going to accelerate. Ensuring the security of information on the Federal government's networks and systems will remain a core focus of the Administration as we move aggressively to implement innovative protections and respond quickly to new challenges as they arise. In addition to the actions we are taking, we also look forward to working with Congress on legislative actions that may further protect our nation's critical networks and systems.

I thank the Committee for holding this hearing, and for your commitment to improving Federal cybersecurity. I would be pleased to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

Ms. Burns, you are now recognized for five minutes.

STATEMENT OF SYLVIA BURNS

Ms. BURNS. Thank you. Good morning, Chairman Chaffetz, Ranking Member Cummings, and distinguished members of the committee. My name is Sylvia Burns and I am the Chief Information Officer for the U.S. Department of the Interior. I appreciate the opportunity to testify regarding DOI's efforts to secure and protect agency, customer, and employee data in the wake of recently discovered cyber intrusion.

Additionally, we appreciate having had the opportunity to provide a classified briefing on the cyber intrusion for members of your committee staff and other congressional staff on May 21st, 2015.

Cyber intruders executed very sophisticated tactics to obtain unauthorized access to OPM data hosted in a DOI data center which contained sensitive personally identifiable information. The incident was and remains under active investigation. At present, the effort has not discovered evidence that any data other than OPM data was exfiltrated.

DOI has initiated a major planning effort to address short, medium and long-term remediation to strengthen our security protections and reduce risks to the Department, our employees, our customers, and our partners. DOI takes the privacy and security of this data very seriously.

In April, DHS's U.S. Computer Emergency Readiness Team, US–CERT, informed DOI about a potential malicious activity which was later determined to be a sophisticated intrusion on DOI's network. DOI immediately began working with US–CERT, the FBI, and other Federal agencies to initiate an investigation and determine what information may have been compromised. DOI allowed DHS and the other investigating agencies immediate access to the DOI computer systems and DOI dedicated people to support the investigation.

Although there is evidence that the adversary had access to the DOI data center's overall environment, today the investigation has not discovered evidence that any data other than OPM data was exfiltrated. However, the investigation remains ongoing.

Concurrent with the investigation, DOI immediately initiated a major planning effort to address short, medium and long-term remediation to strengthen our cybersecurity protections. We undertook those efforts in the context of other cybersecurity improvements which were already underway pursuant to the Department's commitment to the Administration's cybersecurity cross-agency priority goals, as well as DHS's CDM program. We have now accelerated our work on preexisting efforts while devising and implementing new security measures in consultation with the investigating agencies with the expertise related to this particular threat.

Activities underway include working with DHS to scan for specific malicious indicators across the entire DOI network. As part of DHS's binding operational directive, we are identifying and mitigating critical IT security vulnerabilities for all internet-facing systems, and at the direction of the Secretary and Deputy Secretary

we are doing the same for all of DOI's IT systems. This includes systems that are for DOI's internal use as well as systems for the public and non-DOI users.

We are acquiring and implementing new capabilities that will help us to detect and respond quickly to new intrusions. We continue to meet with interagency partners to learn about their activities and leverage their knowledge to make additional improvements to our cybersecurity posture at DOI. We are fully enabling two-factor authentication for all users.

DOI's existing long-term plan includes several agency-wide strategic initiatives, including continuing our commitment to DHS's CDM program. We are almost done implementing hardware and software asset management, and we will be adding new capabilities for application whitelisting, network access control, and dashboarding functionality to provide a comprehensive view of the Department's security posture.

We are strengthening DOI's cybersecurity and privacy workforce so that we have knowledgeable and experienced people to address current and future threats facing the agency. We are designing and implementing increased network segmentation so that, if an intrusion occurs within one component of our network, we can better limit the extent of the exposure. We are evaluating data protection technologies, such as information rights management, for potential future investments.

Again, DOI takes the privacy and security of its data very seriously. We are committed to supporting and continuing the investigation regarding the incident affecting OPM data. Furthermore, we will continue to be an active participant in the ongoing efforts by the Federal Government to improve our Nation's overall cybersecurity posture.

Chairman Chaffetz, Ranking Member Cummings, and members of the committee, this concludes my prepared statement. I would be happy to answer any questions that you may have.

[Prepared statement of Ms. Burns follows:]

Good afternoon Chairman Chaffetz, Ranking Member Cummings, and distinguished members of the Committee. My name is Sylvia Burns and I currently serve as the Chief Information Officer (CIO) for the U.S. Department of the Interior (DOI). We appreciate the opportunity to testify regarding DOI's efforts to secure and protect agency, customer and employee data in the wake of the recently discovered cyber intrusion. Additionally, we appreciate having had the opportunity to provide a classified briefing on the cyber intrusion for members of your Committee staff, and other congressional staff, on May 21, 2015.

Cyber intruders executed very sophisticated tactics to obtain unauthorized access to Office of Personnel Management (OPM) data, hosted in a DOI data center, which contains sensitive personally identifiable information (PII). This incident was, and remains under active and ongoing investigation. At present, the investigation has not discovered evidence that any data, other than OPM data, was exfiltrated.

Concurrent with the ongoing investigation, DOI initiated a major planning effort to address short, medium and long-term remediation in order to strengthen our security protections and reduce risks to the Department, our employees, our customers and our partners. DOI takes the privacy and security of this data very seriously. We are working to support the current investigation regarding the incident affecting OPM data and to minimize the risk of future intrusions and their potential impact.

Background

In April, the Department of Homeland Security's (DHS) U.S. Computer Emergency Readiness Team (US-CERT) informed DOI about potential malicious activity, which was later determined to be an advanced persistent threat, on DOI's network.

As soon as DOI became aware of the suspicious activity, we began working with US-CERT, the Federal Bureau of Investigation (FBI) and other Federal agencies to initiate an investigation and determine what information may have been compromised. DOI allowed DHS and the other investigating agencies immediate access to the DOI's computer systems, and DOI dedicated staff to support the investigation.

Although, there is evidence that the adversary had access to the DOI data center's overall environment, today the investigation has not discovered evidence that any data, other than OPM data, was exfiltrated. It should be noted that DOI also performs shared services for other agencies. The investigation has not discovered evidence that any of its shared service customer data was exfiltrated. However, the investigation remains ongoing.

Remediation

Concurrent with the ongoing investigation, DOI immediately initiated a major planning effort to address short, medium and long-term remediation to strengthen our cybersecurity protections. We undertook those efforts in the context of other cybersecurity improvements, which were already underway pursuant to the Department's commitment to the Administration's cybersecurity cross agency priority (CAP) goals, as well as DHS's continuous diagnostics and mitigation (CDM) program. We have now accelerated our work on some of those activities, while also devising and implementing other security measures with the advice, guidance and consultation of investigating agencies with expertise related to this particular threat.

DOI is currently employing a comprehensive, multi-pronged remediation strategy to prevent, detect and act against malicious activity on our network in order to respond and recover following an incident. Central to this effort are measures to protect the data of our employees, customers and partners.

Activities that are underway include:

- We are working with DHS and our bureaus and offices to scan for malicious indicators across the entire DOI network.
- As part of DHS's Binding Operational Directive (BOD) we are identifying and mitigating critical Information Technology (IT) security vulnerabilities for all internet facing systems.
- The Secretary and Deputy Secretary expanded on DHS's BOD by directing my office – the Office of the Chief Information Officer (OCIO) – to take the lead in mitigating critical vulnerabilities for all of DOI's IT systems.
- We are acquiring and implementing new capabilities that will help us to detect and respond quickly to new intrusions. We continue to meet with interagency partners to learn about their activities and leverage that knowledge to continue to make additional improvements to our cyber security posture at DOI.
- We are fully enabling two factor authentication for privileged users (e.g., system administrators, etc.), as well as regular end-users.

DOI's existing long-term plans include several agency-wide strategic initiatives. For example, DOI is continuing its commitment to DHS's CDM program, which includes meeting our goal to complete the first round of activities around implementing hardware and software asset management. We are entering the second phase of DHS's CDM program activities. This will give DOI the ability to do application whitelisting, network access control to hardware, and dashboarding functionality to provide a comprehensive view of the Department's security posture.

Another important component of our long-term strategic plan includes strengthening DOI's cybersecurity and privacy workforce so that we have knowledgeable and experienced people to address current and future threats facing the agency. Having enough capable and dedicated cybersecurity, privacy and IT operations staff is critical to responding to threats and incidents, and sustaining normal operations following an intrusion.

Additionally, we are designing and implementing increased network segmentation so that, if an intrusion occurs within one component of our network, we can better limit the extent of the potential exposure. We are also evaluating data protection technologies such as information rights management for potential future investments. This will likely drive the modernization of legacy IT systems that cannot currently support data protections.

Conclusion

Again, DOI takes the privacy and security of its data very seriously. We are committed to supporting the continuing investigation regarding this incident affecting OPM data. Furthermore, we will continue to be an active participant in the ongoing efforts by the Federal government to improve our nation's overall cybersecurity posture.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my prepared statement. I would be happy to answer any questions that you may have.

Chairman CHAFFETZ. Thank you.

Ms. Seymour, you are now recognized for five minutes.

STATEMENT OF DONNA K. SEYMOUR

Ms. SEYMOUR. My remarks were included with the Director. Thank you for having me here today, Chairman Chaffetz and Ranking Member Cummings, and I will be happy to answer questions.

Chairman CHAFFETZ. Mr. Esser, you are now recognized for five minutes.

STATEMENT OF MICHAEL R. ESSER

Mr. ESSER. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, good morning. My name is Michael R. Esser. I am the Assistant Inspector General for Audits at U.S. Office of Personnel Management.

Thank you for inviting me to testify at today's hearing on the IT security audit work performed by the OPM Office of the Inspector General.

Today I will be discussing OPM's long history of systemic failures to properly manage its IT infrastructure, which we believe ultimately led to the breaches we are discussing today.

There are three primary areas of concern that we have identified through our 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 offices managing their IT systems. The agency's CIO had ultimate responsibility for protecting these systems, but often did not have the access or control to do so. The program office staff responsible for IT security frequently had no IT background and performed this function in addition to their other full-time roles.

As a result of this decentralized structure, many security controls remained unimplemented or untested, and all of our FISMA audits between 2007 and 2013 identified this as a serious concern.

However, in 2014, OPM took steps to centralize IT security responsibility with the CIO. This new structure has resulted in improvement in the consistency and quality of security practices at OPM. Although we are optimistic about these improvements, it is apparent that the OCIO is still negatively impacted by years of decentralization.

The second topic is security assessments and authorization. This is a comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate.

OPM has a long history of issues related to system authorization as well. In 2010 and 2011 we noted serious concerns in this area, but, after improvements were made, 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. Recently, the OCIO has temporarily put authorization efforts on hold while it modernized OPM's IT infrastructure in response to security breaches, and so it is likely that the number will increase. While we support the effort to modernize systems, we believe that authorization activities should continue.

The third topic 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. However, such tools are only helpful if they are used properly and cover the entire technical infrastructure. We have concerns that they are not.

For example, we were told that OPM performs vulnerability scans on all computer servers using automated scanning tools. Although OPM was performing the scans, our audit also found that some were not done correctly and that some servers were not scanned at all.

One significant control that is lacking altogether is the requirement for PIV credentials for two-factor authentication to access information systems. We also determined that OPM does not have an accurate centralized inventory of all servers and databases. Even if all OPM security tools were being used properly, OPM cannot fully defend its network without a comprehensive list of assets.

In closing, it is clear that even though security responsibility is now highly centralized under the OCIO, the recent security breaches indicate that OPM still has significant work to do to identify all of the assets and data that it is tasked with protecting and then take the steps to do so.

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

[Prepared statement of Mr. Esser follows:]

Office of the Inspector General
United States Office of Personnel Management

Statement of
Michael R. Esser
Assistant Inspector General for Audits

before the

Committee on Oversight and Government Reform

United States House of Representatives

on

"OPM: Data Breach"

June 16, 2015

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

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 on the information technology (IT) security audit work performed by the OPM Office of the Inspector General (OIG). Specifically, today I will be discussing the audits that our office has performed under the Federal Information Security Management Act, commonly known as "FISMA." As I will describe, some of the issues identified in these audits date back to Fiscal Year (FY) 2007.

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 be discussing three of the most significant issues identified in our FY 2014 FISMA audit.

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.

In the FY 2007 FISMA report, we identified a material weakness[1] related to the lack of IT security policies and procedures. In FY 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT security policies. Although OPM's Office of the Chief Information Officer (OCIO) was responsible for the agency's overall technical infrastructure, each OPM program office had primary responsibility for managing its own IT systems. 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. The agency had not clearly defined which elements of IT security were the responsibility of the program offices, and which were the responsibility of the OCIO.

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 FY 2013.

However, in FY 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. Specifically, in FY 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 FY 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.

We have observed that 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. Although the IT security business processes are becoming more centralized under the CIO, the technical infrastructure remains fragmented and therefore inherently difficult to protect.

---

[1] An IT material weakness is a severe control deficiency that prohibits the organization from adequately protecting its data.

2. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) is a comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment. The Office of Management and Budget (OMB) mandates that all Federal information systems have a valid Authorization.

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

However, problems with OPM's system Authorizations have recently resurfaced. In FY 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.[2] 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. The OCIO has temporarily put Authorization efforts on hold while it modernizes OPM's IT infrastructure in response to security breaches. We support the OCIO's effort to modernize its systems, but we believe that Authorization activity should continue, as the modernization is likely to be a long-term effort.

We believe that one of the core causes of these frequent delays in completing the Authorization packages is that there are currently no consequences for the owners of OPM IT systems that do not have a valid Authorization to operate. Although 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. Perhaps the most effective way to reduce delays would be to introduce administrative sanctions for 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,[3] we also recommended that

---

[2] The OIG is the co-owner of one of these IT systems, along with OPM's Healthcare and Insurance (HI) and the Office of the Chief Financial Officer (OCFO), and the system is hosted by the OCIO. The system is the Audit Report and Receivables Tracking System, used to track the resolution of OIG audit recommendations, both procedural and monetary. The system does not collect or maintain any personally identifiable information. The OIG is working with HI, OCFO, and OCIO to resolve any issues.

[3] We acknowledge that OMB now allows agencies to make ongoing Authorization decisions for IT systems based on the continuous monitoring of security controls – rather than enforcing a static, three-year re-Authorization process. However, OPM has not yet developed a mature continuous monitoring program. Until such a program is in place, we continue to expect OPM to re-authorize all of its IT systems every three years.

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.

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

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

In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency's network. As of the end of FY 2014, over 95 percent of OPM workstations required PIV authentication to access the OPM network. However, none of the agency's 47 major applications require 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.

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. Again, of particular concern is the high number of IT systems that are currently operating without a valid Authorization.

We acknowledge that OPM participates in multiple Government-wide security programs. However, these programs are designed to complement, not replace, a comprehensive IT security program. It is critical that OPM take steps to secure its network from within, and our audit recommendations are designed to help them do so.

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

Chairman CHAFFETZ. Thank you.

We now recognize the ranking member, Mr. Cummings of Maryland, for five minutes.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

The recent cyber attack against the Office of Personnel Management is the latest in a series of aggressive attacks against our Nation in both the public and private sectors.

I want to put up a slide that lists some of the most significant breaches over the past few years.

[Slide shown.]

Mr. CUMMINGS. Anthem, 80 million people; JPMorgan, 76 million people; Target, 70 million people; OPM, at least 4 million so far. Then there was the Postal Service, Sony Pictures, and USIS. This is not a comprehensive list by any means.

Ladies and gentlemen, when you see this list, the picture is clear: the United States of America is under attack. Sophisticated cyber spies, many from foreign countries, are targeting the sensitive personal information of millions, millions of Americans. They are attacking our government, our economy, our financial sector, our healthcare system, and virtually every single aspect of our lives.

For more than two years I have been pressing for our committee to investigate these cyber attacks, so I thank the chairman for holding today's hearing, and I hope we will hold similar hearings on many of these other attacks as well.

With respect to the attack against OPM, my primary concern is who was targeted, government workers, and what foreign governments could do with this information. I have several questions for OPM.

How many Federal employees were indeed affected? What kind of information was compromised? And what steps are being taken to help these employees now? I also want to know how these attackers got inside of OPM's networks.

Last year, cyber attackers penetrated the networks of USIS and Keypoint, two contractors that perform background checks for security clearances on behalf of OPM.

One of the most critical questions we have today is, did these cyber attackers gain access to OPM's data systems using information they stole from USIS or Keypoint last year. Did they get the keys to OPM's network from one of its contractors?

Mr. Chairman, I asked you to invite both Keypoint and USIS representatives here to testify today. You agreed to invite USIS, but last night they refused, just as they have refused repeated requests for information over the past year. They did not offer someone else they thought would be appropriate; they simply refused.

I do not say this lightly, Mr. Chairman, but I believe USIS and its parent company may now be obstructing this committee's work. We have suggested previously that the committee hold a transcribed interview. Given the history of noncompliance at USIS, I believe this may be one of the only ways to obtain the information we are seeking.

Mr. Chairman, over the past two years I have also been pressing to investigate ways to better protect personal information that belongs to the American people: their financial records, their medical

records, their credit card information, their Social Security numbers, and a host of other information they want to keep secure.

I sought advice from some of the Nation's top information security experts in private business and government. These experts warn that we cannot rely primarily on keeping the attackers out. We need to operate with the assumption that the attackers are already inside. They are already there.

Last week, one of the world's foremost cybersecurity firms, Kaspersky Labs, was penetrated in a cyber attack, and, according to FireEye, one of the companies my staff spoke with, the average amount of time a hacker remains undetected is more than 200 days. That is a lot of time.

Obviously, we need strong firewalls and other defenses to keep attackers out. But experts recommend much more aggressive measures to wall off or segregate data systems to minimize the impact of inevitable data breaches in the future. Practices like data masking, redaction and encryption must become the norm rather than the exception.

Finally, we need to remember who the bad guys are here. They are not U.S. companies or Federal workers who are trying to keep our information safe. The bad guys are the foreign nations and other entities behind these devastating attacks.

According to law enforcement officials, North Korea, China, Russia, and Iran are the most advanced persistent threats to this Nation's cybersecurity. So, as we move forward today, I want to caution everyone that as much as we want to learn about this attack, we have to do so in a responsible way. A lot of the information about the attack is classified, and the last thing we want to do is give our enemies information or compromise active law enforcement investigations.

We are having a classified briefing for members at 1:00 p.m. today, so I encourage everyone to attend.

As I close, Mr. Chairman, I want to thank you again for the bipartisan approach that you have taken on this issue, and I hope we can continue to investigate these and other breaches to identify common threats against our Country and the best ways to counter them.

With that, I yield back.

Chairman CHAFFETZ. Thank you.

I now recognize myself for five minutes.

Ms. Archuleta, my question for you is, how big was this attack? How many Federal workers have been compromised? We have heard 4 million, we have heard 14 million. What is the right number?

Ms. ARCHULETA. During the course of the ongoing investigation into the cyber intrusion of OPM, the compromise of personnel records of current and former Federal employees that we announced last week, that number is approximately 4.2 million. In addition, in the investigation of that breach, we discovered, as I mentioned in my testimony, an additional OPM system was compromised, and these systems included information based on the background investigations of current, former, and prospective Federal Government employees, as well as other individuals.

Because different agencies feed into OPM background investigation systems in different ways, we are working with the agencies right now to determine how many of their employees were affected. We do not have that number at this time, but we will get back to you once we have more information.

Chairman CHAFFETZ. What is your best estimate? Is the 14 million wrong or accurate?

Ms. ARCHULETA. As I said before, we do not have an estimate because this is an ongoing investigation.

Chairman CHAFFETZ. How far back does it go? You are talking about former employees, current employees, and potential employees, so how far back does this information go that was in your system?

Ms. ARCHULETA. Thank you for that question, Mr. Chaffetz. I would have to respond again because it is an ongoing investigation——

Chairman CHAFFETZ. It has nothing to do with impeding an investigation. You should know what information you have and what you don't. So this is not going to slow down any investigation. People have a right to know. The employees have a right to know. How far back does your information and database go that was compromised?

Ms. ARCHULETA. The legacy systems date back to 1985, but I do not——

Chairman CHAFFETZ. So anything that is 1985——

Ms. ARCHULETA. No, sir, that would not be correct.

Chairman CHAFFETZ. You don't know. Does it include military personnel?

Ms. ARCHULETA. As I said, this is an ongoing investigation.

Chairman CHAFFETZ. It is a yes or no question. Does it include military personnel?

Ms. ARCHULETA. I would be glad to discuss that in a classified setting.

Chairman CHAFFETZ. Does it include contractor information?

Ms. ARCHULETA. Again, I would be glad to discuss that in a classified setting.

Chairman CHAFFETZ. There is nothing classified as to what information this includes. Does it include CIA personnel?

Ms. ARCHULETA. I would be glad to discuss that in a classified setting.

Chairman CHAFFETZ. Does it include anybody who has filled out SF 86, the Standard Form 86?

Ms. ARCHULETA. The individuals who have completed an SF 86 may be included in that, and we can provide additional information in a classified setting.

Chairman CHAFFETZ. Why wasn't this information encrypted?

Ms. ARCHULETA. The encryption is one of the many tools that systems can use. I will look to my colleagues at DHS for their response.

Chairman CHAFFETZ. No, I want to know from you why the information wasn't encrypted. This is personal, sensitive information; birth dates, Social Security numbers, background information, addresses. Why wasn't it encrypted?

Ms. ARCHULETA. Data information encryption is valuable——

Chairman CHAFFETZ. Yeah, it is valuable. Why wasn't it?

Ms. ARCHULETA.—and is an industry best practice. In fact, our cybersecurity framework promotes encryption as a key protection method.

Chairman CHAFFETZ. Why didn't you——

Ms. ARCHULETA. Accordingly, OPM does utilize encryption——

Chairman CHAFFETZ. We didn't ask you to come read statements. I want to know why you didn't encrypt the information.

Ms. ARCHULETA. An adversary possessing proper credentials can often decrypt data. It is not feasible to implement on networks that are too old. The limitations on encryptions are effectiveness is why OPM is taking other steps such as limiting administrator's accounts and requiring multi-factor authentication.

Chairman CHAFFETZ. Okay, well, it didn't work, so you failed. Okay? You failed utterly and totally. So the inspector general, November 12th, 2014, we recommend that the OPM director consider shutting down information systems that do not have current and valid authorization, and you chose not to. Why?

Ms. ARCHULETA. I appreciate the report by the IG. We work very closely with our IG and take very seriously——

Chairman CHAFFETZ. Okay, but he had a very serious recommendation to shut down the system. That is how bad it was. And you said no.

Ms. ARCHULETA. I would like to turn that over to my colleague.

Chairman CHAFFETZ. No, I would like you to answer that question. It says we recommend that the OPM director consider shutting it down. Your response back from the Office of Chief Information Officer, "The IT program managers will work with the ISSOs to ensure that OPM systems maintain current ATOs and that there are no interruptions to OPM's mission operation." Basically, you said no.

The inspector general was right. Your systems were vulnerable. The data was not encrypted. It could be compromised. They were right last year. They recommended, it was so bad, that you shut it down, and you didn't, and I want to know why.

Ms. ARCHULETA. There are many responsibilities we have with our data, and to shut down the system we need to consider all of the responsibilities we have with the use of our systems.

Chairman CHAFFETZ. So you made a conscious decision knowing that it was vulnerable, that all these millions of records of Federal employees was out there? The inspector general pointed out the vulnerability and you said no, we are not making a change.

Ms. ARCHULETA. As the director of OPM, I have to take into consideration all of the work that we must do. It was my decision that we would not, but continue to develop the system and making sure that we have the security within those systems.

Chairman CHAFFETZ. And did you do that? You didn't. You didn't, did you? That didn't happen, did it?

Ms. ARCHULETA. The recommendation to close down our systems came after the adversaries were already in our network.

Chairman CHAFFETZ. When did they get in network?

Ms. ARCHULETA. It was as a result of our security systems that we were able to detect this intrusion.

Chairman CHAFFETZ. When did they get into the system?

Ms. ARCHULETA. We detected the intrusion in April.

Chairman CHAFFETZ. Of?

Ms. ARCHULETA. Of 2015.

Chairman CHAFFETZ. But in November 2014 you didn't know if they were in there, did you?

Ms. ARCHULETA. No, we did not. We did not have the security systems installed at that time. It was because we were able to add those security systems that we were able to detect.

Chairman CHAFFETZ. So you detected the system? It wasn't a software provider? You found it yourself?

Ms. ARCHULETA. OPM detected the intrusion.

Chairman CHAFFETZ. So The New York Times and the others who wrote that were wrong?

Ms. ARCHULETA. That is correct.

Chairman CHAFFETZ. Two more questions, with your indulgence here. How many people have received letters?

Ms. ARCHULETA. There is a rolling number as we work from the first date of notification, January 8th, we will complete the notification to 4.2 million by June 19th. I am sorry I don't have the exact number as of today. I would be glad to get that information for you.

Chairman CHAFFETZ. One last question, with everybody's indulgence here.

Ms. Archuleta, there was a data breach at OPM in July of 2014, okay? This is what you said about Ms. Seymour. In December, I was very fortunate to bring Donna Seymour, from the Department of Defense, onboard. She has great experience with the IT world and has brought her talents to OPM. It was because of her leadership and her dedicated employees that we were able to make sure that none of this personal identifiable information was compromised.

This was July of 2014. You cited her and the data breach as making sure that none of the personal identifiable information got out the door. Now that it has been hacked, are you going to give her that same amount of credit?

Ms. ARCHULETA. I do give her that same amount of credit, sir. When I began my tenure as the Director of OPM, one of my first priorities was to develop an IT strategic plan and to develop the important pillar of cybersecurity within our systems. We have worked very hard since that time, and as we update these legacy systems it is important that we recognize that there is a persistent and aggressive effort on the part of these actors to not only intrude in our system, but systems throughout government and, indeed, in the private sector.

Chairman CHAFFETZ. Well, you have completely and utterly failed in that mission if that was your objective. The inspector general has been warning about this since 2007. There has been breach after breach. He recommended shutting it down last year and you, you made a conscious decision to not do that. You kept it open. The information was vulnerable and the hackers got it.

I don't know if it was the Chinese, the Russians, or whoever else, but they have it, and they are going to prey upon the American people. That is their goal and objective, and you made a conscious decision to leave that information vulnerable. It was the wrong de-

cision. It was in direct contradiction to what the inspector general said should happen, and he had been warning about it for years.

Ms. ARCHULETA. I would note that in the IG's report that he acknowledges the fact that we have taken important steps in reforming our IT systems. Advanced tools take time.

Chairman CHAFFETZ. So what kind of grade would you give yourself? Are you succeeding or failing?

Ms. ARCHULETA. Cybersecurity problems take decades.

Chairman CHAFFETZ. We don't have decades. They don't take decades.

Ms. ARCHULETA. I am sorry, cybersecurity problems are decades in the making. The whole of government is responsible, and it will take all of us to solve the issue and continue to work on them. My leadership with OPM is one that instigated the improvements and changes that recognized the attack.

Chairman CHAFFETZ. I yield back.

I recognize the ranking member, Mr. Cummings, for as much time as he wants.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Ms. Seymour, this data breach is particularly concerning because the individuals who were targeted were government employees and the suspected attackers are foreign entities. I am concerned that this breach may pose a national security threat.

According to a statement from OPM, the personal information of approximately 4 million current and former Federal employees was compromised in this breach. What can you tell us about the type of personal information that was compromised in this breach?

Ms. SEYMOUR. Thank you for the question, sir. The type of information involved in the personal records breach includes typical information about job assignments, some performance ratings, not evaluations, but performance ratings, as well as training records for our personnel. The information involved in the background investigations incident involves SF 86 data, as well as clearance adjudication information.

Mr. CUMMINGS. So, Social Security numbers?

Ms. SEYMOUR. Yes, sir. Social Security number, date of birth, place of birth; typical PII that would be in those types of files.

Mr. CUMMINGS. Ms. Seymour, it was reported on Friday that, in addition to this breach, hackers had breached highly sensitive information gathered in background investigations of current and former Federal employees. Is that true?

Ms. SEYMOUR. Yes, sir, that is.

Mr. CUMMINGS. Do you know how far back that goes?

Ms. SEYMOUR. No, sir, I don't. The issue is that these are longitudinal records, so they span an employee's career. So I do not know what the oldest record is.

Mr. CUMMINGS. So it is possible that somebody could be working for the Federal Government for 30 years and that their information over that 30 years could have been breached?

Ms. SEYMOUR. Yes, sir, these records do span an employee's career.

Mr. CUMMINGS. So what can you tell us about the type of information that may have been compromised in the second breach?

Ms. SEYMOUR. I believe that that would be a discussion that would be better had in our classified session this afternoon, sir.

Mr. CUMMINGS. Thank you. I am going to come back to you.

Dr. Ozment, these suspected cyber spies from a foreign state went after sensitive detailed information about Federal employees. What could they do with this information? I am talking to you, yes.

Mr. OZMENT. Ranking member, I am going to have to defer that question to the intelligence community, who will be a participant in our classified briefing this afternoon at 1:00.

Mr. CUMMINGS. All right.

Experts advise taking steps to mitigate damage from cyber spying attacks by using tools such as data segmentation, data masking, and encryption; and the chairman asked about encryption. I know from past OPM testimony before the committee that OPM has been a leader in deploying those tools.

Now, Ms. Seymour, it is kind of hard to understand how cyber spies could have accessed more than 4 million records if you were using those tools to the fullest. Ms. Archuleta has a lot of faith and confidence in you, as the chairman just stated. Can you explain what happened?

Ms. SEYMOUR. Thank you, Mr. Cummings, for the question. A lot of our systems are aged, and implementing some of these tools take time, and some of them we cannot even implement in our current environment. That is why, under Director Archuleta's leadership, we have launched a new program where we are building a new environment, a new architecture, a modern architecture that allows us to implement additional security features.

In our legacy environment, we have installed numerous technologies, and that is how we discovered this breach in the first place. So we are shoring up what we have today, and then we are building for the future so that we can become more secure and provide these types of protections to our data and our systems.

Mr. CUMMINGS. Well, in the meantime, if we are going to collect and we are going to store sensitive personal information, we must make it unusable to our adversaries, if they are cyber spies, are able to steal it. Would you agree? OPM, as well as American businesses, have to do a better job of protecting sensitive information. Would you agree, ma'am?

Ms. SEYMOUR. Yes, sir.

Mr. CUMMINGS. Now, Ms. Seymour, do you have the tools now to do that? Are you trying to tell us you don't?

Mr. SEYMOUR. OPM has procured the tools, both for encryption of its databases, and we are in the process of applying those tools within our environment. But there are some of our legacy systems that may not be capable of accepting those types of encryption in the environment that they exist in today, and that is why it is important for us to focus very aggressively, very proactively on building out that new architecture so that, in the future, we will be able to implement those tools for all of our databases.

Mr. CUMMINGS. Now, when you talk about the future, I mean, what are you talking about? Are you talking about three months, three years?

Ms. SEYMOUR. We began our program after the March 2014 incident. We worked very closely with our interagency partners to de-

vise a very aggressive and very comprehensive plan. We have been implementing that plan since then. We are delivering what we call our shell, which is the new architecture, we are delivering that this fall and we will begin looking at our business systems applications and how we can migrate those into the new architecture.

Mr. CUMMINGS. Ms. Seymour, this is the question: We are collecting data right now. There is people's data that is out there. And I am talking about, in the meantime, where are we? In other words, I know you are trying to do some things, but that doesn't make Federal employees feel pretty good. It doesn't make me feel good.

So tell me more. Are you saying that we are just vulnerable and we don't know when we are going to be able to deploy the types of systems that you just talked about?

Ms. SEYMOUR. No, sir. We have done a number of things.

Mr. CUMMINGS. I am not talking about what you have done. I am talking about what is going on today.

Ms. SEYMOUR. That is exactly what I am offering, sir.

Mr. CUMMINGS. All right.

Ms. SEYMOUR. We have implemented two-factor authentication for remote access to our network. That means that without a PIV card or some other type of device that our users cannot log into our network remotely. We have implemented additional firewalls in our network. We have tightened the settings of those firewalls. We have reduced the number of privileged users in our account and we have even further restricted the access privileges that those users have.

We have made a number of other steps to increase the security of our existing network. We began that work back last March and it has continued, and we continue to work with DHS and our agency partners to test those systems and make sure that they are working appropriately.

Mr. CUMMINGS. Now, Mr. Esser, the Office of Inspector General conducted an audit in 2014, the chairman was talking about this, of OPM's information security programs and found several weaknesses. Can you briefly identify what those weaknesses were that you found?

Mr. ESSER. Yes, sir. The most critical weaknesses that we identified in our FISMA report from 2014 were the continued information security governance problems that have existed since 2007, the decentralization of the controls over systems. That, however, is an area that is certainly close to being improved to a full extent.

Another area of weaknesses were the security assessments and authorization, which is each system that OPM owns should go under an assessment every three years and be authorized for usage. We identified 11 systems at the end of 2014 that had not been authorized that were due to be authorized.

The technical security controls was another big area that we identified. While OPM has implemented a number of strong tools and is improving in that area, our concern is that some of those tools were not being used properly and that they do not have a complete and accurate inventory of databases and servers that those tools should be applied against.

Mr. CUMMINGS. So the chairman asked Ms. Archuleta a question of how she thought she'd done. Based upon that, what grade would you give?

Mr. ESSER. I don't know that I could give a grade.

Mr. CUMMINGS. So of all the things that you just stated, there are certain things that were not done, is that right?

Mr. ESSER. Yes, sir.

Mr. CUMMINGS. Did any of them lead to this breach, the things that were not done?

Mr. ESSER. I don't know the exact details of how this breach occurred, so I really can't answer that question. Certainly there are a lot of weaknesses at OPM that they are in the process of trying to address.

Mr. CUMMINGS. And last, but not least, do you have a silver bullet to address this issue, sir?

Mr. ESSER. No, sir, I do not. There are very sophisticated attackers out there and there is no one silver bullet I think that can be applied that will prevent these types of things from happening.

Mr. CUMMINGS. You heard me asking Ms. Seymour about the fact that we are constantly collecting information, and it seems as if we are just vulnerable and that there are certain areas that we may not be able to defend ourselves in. Is that an accurate statement?

Mr. ESSER. Certainly, there are a lot of things that can be done to make our systems more secure. Is there something that can be done to make them impenetrable? Not that I am aware of.

Mr. CUMMINGS. Thank you very much.

Chairman CHAFFETZ. I now recognize the gentleman from Michigan, Mr. Walberg, for five minutes.

Mr. WALBERG. Thank you, Mr. Chairman. I appreciate the witnesses being here.

This morning we have certainly heard that there is no silver bullet, and I don't think we expected the answer to be, yes, there is a silver bullet. We are concerned that, knowing what has been going on, having clear evidence that hackers have been attempting for quite some time and then, at least those of us here who trust on agencies and people like yourselves who know the issues, that some more efforts could have been successful in stopping the most recent attacks.

We have heard today that networks aren't compartmentalized, segmented, in certain cases encrypted; that with the recent attacks, exterior perimeter has been breached, the attacker often remains undetected for months. That is concerning. As a result of that, able to exploit vulnerabilities within the networks without passing through, and this is most concerning to me, additional inspection or security measures.

So, Mr. Scott, as I understand, in the private sectors there have been shifts towards zero trust model. Ultimately, given OMB's role in setting metrics for agencies, my question is can you tell me, tell us what OMB is doing to set IT security metrics to limit the number of workloads, application tiers to the networks?

Mr. SCOTT. Thank you for the question.

I think there are a number of things that I would point to in addition to the measures that you just talked about. The first one is to share across the Federal Government not only the lessons learned from OPM, but what we see from other attacks, whether successful or not, private and public, and make sure that all agencies are up to speed with the latest information on the methods of attack, the tools that are used, and so on.

Mr. WALBERG. That is a weakness right now, is what you are telling me, that that is not happening?

Mr. SCOTT. It has been historically. The ability for the Government and the private sector to share information has been a hindrance in our ability to thwart these things.

But I will say that the specific measure that you mentioned, the segmentation and zero trust, is something that is more easily applied to very modern architectures. It is not as easily applied to some of the oldest and old legacy systems that we have. And I think that is going to be a challenge for all agencies where the architecture itself just doesn't lend itself to the application of certain technologies.

The best answer, I think, in terms of what we have and where we go is a model that we are promoting and encouraging across the agencies, which is defense in depth. It is a number of different measures to that if one thing doesn't work, you have the next layer that helps; and if that doesn't work, you have the next layer. And zero trust is applicable in some of those environments and, frankly, is very difficult or impossible to apply in others.

Mr. WALBERG. How far are we from that?

Mr. SCOTT. I would say years and years comprehensively. But one of the things that we are working on right now is prioritizing based on the highest value assets that the Federal Government has so that we are going after the most valuable stuff first and make sure that is protected the best way we can.

Mr. WALBERG. Ms. Seymour, with the millions of current and former Federal employees, a lot of them in my district, that sign on to do the work that we give to them, we appreciate the work, it is not something they make up. We ask them to do the Federal jobs that the agencies, the departments that they work under have been asked to do. They don't expect that their life will be compromised, their history will be compromised, their records be compromised.

When did OPM begin letting victims know of the breach and the risk to their identities?

Ms. SEYMOUR. Thank you for your question, sir. I too am a Federal employee and very concerned about this matter; it is grave and serious, so I appreciate that.

We began notifying personnel on June 8th, and will continue to make those notifications through June 19th. That is for the personnel records security incident that we have.

We have not yet been able to do the analysis of the data that is involved with the background investigations incident. That is ongoing, and as soon as we can narrow the data that is involved in that incident, we will make appropriate notifications for that one as well.

Mr. WALBERG. Okay. Thank you.

Chairman CHAFFETZ. Thank you. I thank the gentleman.

I now recognize the gentlewoman from New York, Mrs. Maloney, for five minutes.

Mrs. MALONEY. I want to thank the chairman and ranking member for calling this hearing, and all of our panelists for your public service.

As one who represents the city that was attacked by 9/11, we lost thousands on that day and thousands more are still dying from health-related causes from that fateful day. But I consider this attack, I call it an attack on our Country, a far more serious one to the national security of our Country.

I would like to ask Mr. Ozment from Homeland Security, would you characterize this as a large-scale cyber spying effort? That is what it sounds like to me. What is it?

Mr. OZMENT. I think to speak to whether or not this was a spying effort, we would have to talk to any understanding of who the adversaries were and what their intent was, and I think that is a conversation better reserved for a couple of hours from now.

Mrs. MALONEY. Do you believe it is a coordinated effort? They appear to be attacking health records, employment records, friendship, family, whole backgrounds. It seems to be a large sphere of information not only from the Government, but private contractors, individuals; and sometimes it appears targeted towards Americans who may be serving overseas in sensitive positions. But would you consider this a coordinated effort? Can you answer that or is that classified?

Mr. OZMENT. Thank you, Representative. I would defer that question to the classified briefing.

Mrs. MALONEY. Okay. Thank you.

Mr. OZMENT. But what I would say, if you are willing, is that——

Mrs. MALONEY. I will be at the 1:00 meeting. Thank you.

Now, I want to refer to this article, and I would like to place it in the record. I think it is an important one; it came from ABC News.

If I could put it in the record.

Chairman CHAFFETZ. Without objection, so ordered.

Mrs. MALONEY. It reports that there seems to be looking at and gathering information on an SF 18 form, which is a Standard Form 18, which is required for any employee seeing classified security clearances, so that would be people in important positions in our Government. And I won't ask any questions on it, I will just wait until later at this classified briefing, but I am extremely disturbed.

This article also points out that it is not only individuals that they are going after; they are going after contractors and those that serve the Government. It mentions in other reports Lockheed Martin, where they went after their secure ID program.

Is that true, Mr. Ozment?

Mr. OZMENT. I can't speak to whether any adversaries have gone after specific private sector companies.

Mrs. MALONEY. Okay. All right. Then we won't get into that.

But other press reports said that there was Northrop Grumman, L3, that they were hit by cyber attacks, and other Government contractors. Now, one that probably hit Congress is one in 2013, where the FBI warned that a group called Anonymous hacked into the

U.S. Army, Department of Energy, Department of Health and Human Services, and many agencies by exploiting a weakness in Adobe systems.

Now, I have the Adobe system in my office, so that means they could have hacked into my office, and probably every other congressional office.

Then they talk about going into healthcare. They go into the Blue Cross Blue Shield system of all the Federal employees. So it seems like they want a comprehensive package on certain millions of Americans, many of whom are serving our Country, I would say at negotiating tables in Commerce, State Department, probably Defense, and every other aspect of American life and the world economy.

But, Mr. Scott, you have been before this committee before and you announced you were going to review the agencies' cybersecurity programs to identify risks and implement gaps. I wonder if you could report on what you learned from this review and any specific changes in cybersecurity policies, procedures, or guidance. If you can report on that. Or that may be classified too. But anything you can share with us on what you have been doing to act to build some firewalls?

Mr. SCOTT. Sure. Well, thank you for the question.

So we are conducting regular CyberStat reviews with each of the agencies, and it is along the key lines of many of the topics we have talked about here: two-factor patching, minimizing the number of system administrators; all of the I will call hygiene factors that we think lead to good cybersecurity.

Mrs. MALONEY. My time has expired, but anything you want to give to the committee in writing, we would appreciate it. Thank you.

Mr. SCOTT. We would be happy to do so. Thank you.

Chairman CHAFFETZ. I thank the gentlewoman.

I ow recognize the gentleman from North Carolina, Mr. Meadows, for five minutes.

Mr. MEADOWS. Thank you, Mr. Chairman.

Ms. Archuleta, let me come to you. You have been in your current position since 2013, is that correct?

Ms. ARCHULETA. I was sworn in in November 2013.

Mr. MEADOWS. So in 2013 you, according to your testimony, made cyber security the highest priority. I think that is how you opened up your testimony, that the security of Federal employees was your highest priority. Is that correct?

Ms. ARCHULETA. Yes, sir.

Mr. MEADOWS. All right. So help me reconcile, then, if it is your highest priority, how, when the most recent IG's report that came out that took security from being a material weakness is how it was characterized before you got there, to significant deficiency, how would you reconcile highest priority and significant deficiency as being one and the same?

Ms. ARCHULETA. Thank you for your question.

As I mentioned earlier, one of the first things that we did, or I did, for OPM was to develop, within 100 days, an IT strategic plan, and the issues that the IG just mentioned, in terms of IT governance and IT leadership, as well as IT architecture, IT agility, IT

data, and IT cybersecurity, were all strong components of this IT plan; and the IG recognized those steps and the strategic plan that we developed.

Mr. MEADOWS. But he did recognize it.

I only have five minutes, so I can't let you just ramble on with all of these things. So let me ask you how, if he recognized that, would he still characterize it as significant deficiencies?

Ms. ARCHULETA. As we were instituting the improvements that we were making, he was also, at the same time, conducting his audit. His audit was conducted in the summer of 2014, when we were beginning to implement our strategic plan, and the IG has continued to work with us and we have taken his recommendations very seriously.

Mr. MEADOWS. You have taken them seriously, so have you implemented all of them? Yes or no? Just yes or no.

Ms. ARCHULETA. We have implemented many of them and are in the process of implementing others.

Mr. MEADOWS. So have you implemented all of those?

Ms. ARCHULETA. As I said, sir, I have implemented many of them and continue to work——

Mr. MEADOWS. So you will implement all of them?

Ms. ARCHULETA. We are looking at each of those recommendations very seriously.

Mr. MEADOWS. Not looking. Will you implement? Can you assure the Federal workers that you are going to implement all the recommendations that the IG recommended to you, yes or no?

Ms. ARCHULETA. We are working very closely with the IG to——

Mr. MEADOWS. I will take that as a no.

All right, so let me go on further, then, because I am very concerned that here we have not even notified most of the Federal employees. We have known about it. They continue to not be notified, and yet here you are saying that you have different priorities. Because when Chairman Chaffetz asked you about why did you not shut it down, you said, well, OPM has a number of other responsibilities. Is that correct? That was your answer to Chairman Chaffetz.

Ms. ARCHULETA. We house a variety of data, not just data on employee personnel files. We also house health care data; we employ other records, and the result——

Mr. MEADOWS. So what you are saying is it was better that you supplied that and put Federal workers at risk versus making it, according to your words, the highest priority to make sure that the information was not compromised. If it is your highest priority, why didn't you shut it down like Mr. Chaffetz asked and like was recommended? Why didn't you shut it down?

Ms. ARCHULETA. In our opinion, we were not able to shut it down in view of all of the responsibilities we hold at OPM. We do take seriously——

Mr. MEADOWS. So, in your opinion, protecting Federal workers then could not have been your highest priority, because there were competing, I guess, priorities, and you said it was better that you continued on with the others versus protecting the Federal workforce.

Ms. ARCHULETA. As I said, the recommendations that the IG gave to us are ones that we take very seriously, sir. I don't want to characterize that we didn't. In fact, we did take them in ongoing conversations.

Mr. MEADOWS. Okay. There is a quote that says what we occasionally have to look at, no matter how beautiful the strategy, we have to occasionally look at the results. And the results here are pretty profound that we have security risks all over. And I would encourage you to take it a little bit more serious and, indeed, make it your highest priority.

I yield back. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank the gentleman.

Now recognize the gentleman from Massachusetts, Mr. Lynch, for five minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

I want to thank our panel for your help.

I want to associate myself with the remarks of the ranking member and the chairman today, which doesn't always happen.

Chairman CHAFFETZ. Duly noted.

Mr. LYNCH. I would like to ask unanimous consent if I might enter into the record the remarks of Colleen M. Kelly, National President of the National Treasury Employees Union, and also a letter from J. David Cox, who is the President of the American Federation of Government Employees, AFL–CIO.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LYNCH. I want to also read the first three paragraphs. This is a letter from the president of the American Federation of Government Employees, AFL–CIO, J. David Cox, to the Honorable Katherine Archuleta.

It says, Dear Honorable Archuleta, I am writing in reference to the data breach announced by the Office of Personnel Management. And this was dated last week. In the days since the breach was announced, very little substantive information has been shared with us, despite the fact that we represent more 670,000 Federal employees in departments and agencies throughout the executive branch.

OPM has attempted to justify the withholding of information on the breach by claiming that the ongoing criminal investigation restricts your ability to inform us of exactly what happened, what vulnerabilities were exploited, who was responsible for the breach, and how damage to affected individuals might be repaired and compensated.

Based on sketchy information that OPM has provided, we believe that the central personnel data file was the targeted database and that the hackers are now in possession of all personnel data for every Federal employee, every Federal retiree, and up to 1 million former Federal employees. We believe the hackers have every affected person's Social Security number, military record, veteran status, address, birth date, job and pay history, health insurance, life insurance, email, pension information, age, gender, race, union status, and a lot more.

Worst of all, we believe the Social Security numbers were not encrypted, a basic cybersecurity failure that is absolutely indefensible and outrageous.

So, Ms. Archuleta, were the Social Security numbers encrypted?

Ms. ARCHULETA. OPM is in the process of——

Mr. LYNCH. Ms. Archuleta, is that an I don't know?

Ms. ARCHULETA. I don't believe that the Social Security——

Mr. LYNCH. Can we just stick to a yes or no?

You know what, this is one of these hearings where I think I am going to know less coming out of this hearing than I did when I walked in because of the obfuscation and the dancing around that we are all doing here.

Matter of fact, I wish that you were as strenuous and hard working at keeping information out of the hands of hackers as you are keeping information out of the hands of Congress and Federal employees. It is ironic. You are doing a great job stonewalling us, but hackers not so much.

So were the Social Security numbers encrypted, yes or no?

Ms. ARCHULETA. No, they were not encrypted.

Mr. LYNCH. There you go. There you go. Now we are getting somewhere.

That is pretty basic, though. That is pretty basic, encrypting Social Security numbers.

So all this happy talk about these complex systems we are going to come up with, you are not even encrypting people's Social Security numbers. That is a shame.

Let me ask you about this Standard Form 86. Now, for those of you, obviously you know that Standard Form 86 is what we require employees to fill out if they are going to receive a security clearance. So these are people who have sensitive information. And we drill down on these folks. This is a copy of the application. It is online if people want to look at it; it is 127 pages online.

And we ask them everything; what kind of underwear they wear, what kind of toothpaste. I mean, it is a deep dive. And that is for a good reason, right? Because we want to know, when people get security clearance, that they are trustworthy. There is information here if you have ever been arrested; your financial information is in here. There is a lot of information in this form.

They hacked this. They hacked this. They got this information on Standard Form 86. So they know all these employees and everything about them that we ask them in the Standard Form 86.

Isn't that right, Ms. Seymour?

Ms. SEYMOUR. I believe that is a discussion that would best be held until this afternoon, sir.

Mr. LYNCH. That is probably a yes.

Like I say, I think you have to be honest with your employees, and I think that, in order to protect them, we need to let them know what is going on, because they have the email addresses in here as well, several, your first, your second, your third email address; and all that information is out there. So we need to be a little bit more, not a little bit more, we need to be more forthcoming with our own employees. These are people who work for us, and a lot of them deserve a lot more protection than they are getting right now from the United States Government and from the Office of Personnel Management.

I see my time has expired. I appreciate the indulgence of the chairman and I yield back.

Chairman CHAFFETZ. I thank the gentleman.

Now we recognize the gentleman from South Carolina, Mr. Mulvaney, for five minutes.

Mr. MULVANEY. Thank you, Mr. Chairman.

Many of us are often uncomfortable asking questions in this type of setting, because obviously we don't want to ask questions the answers to which should be kept confidential. So I encourage you in advance, if I ask you something that we should talk about in a different setting, that is an acceptable answer.

But I sort of feel like in Mr. Lynch in that I don't know if I get my hands around exactly what we are learning. So let's start with this. I am going to follow up on a question that Mr. Meadows asked of Ms. Archuleta, which is, he asked you if you were going to implement all of the IG's recommendations. You said you were working with the IG.

Whether or not that was a yes or no answer, I agree with Mr. Meadows, probably closer to no, so let me address it like this. Can you name for me some of the IG recommendations that you are pushing back against or that you are not interested in implementing?

Ms. ARCHULETA. I don't have the specific recommendations in front of me, and I would be very glad to come back and talk about that.

Mr. MULVANEY. Okay.

Ms. ARCHULETA. But what I would like to say, sir, is that as we look at the recommendations by the IG, we work with him so that he can fully understand where we have moved in our security efforts and also to understand his observations. And that is the normal audit process and we continue to go through that with him and update him on a regular basis.

Mr. MULVANEY. And we get IGs in here all the time and that makes perfect sense. What bugs me, Ms. Archuleta, is that back in the end of 2014 they recommended, in fact, it was their third recommendation, that all active systems in OPM's inventory have a complete and current authorization. Your response to that was saying, "We agree that it is important to maintain up to date and valid ATOs for all systems, but we do not believe that this condition rises to the level of a material weakness."

Do you believe that your opinion on that has changed since November of 2014, Ms. Archuleta?

Ms. ARCHULETA. I appreciate all of the information and the recommendations that the IG has given us, and we will continue to work with him——

Mr. MULVANEY. I didn't ask you that. Do you still believe now, knowing what you know now, that that condition did not rise to the level of material weakness?

Ms. ARCHULETA. Sir, we are working with a legacy system.

Mr. MULVANEY. I didn't ask you that, Ms. Archuleta.

Ms. ARCHULETA. As to the recommendations that he has made to us, we are working through those to the best of our ability.

Mr. MULVANEY. That is what frightens me, Ms. Archuleta, that this is the best of your ability.

Let me see if I can just get some summary information here as I go back and try to explain to folks back home. I have heard that

it was just people in the executive branch. I open this to anybody who might be able to answer this. Are we still saying that the only people whose data was exposed were folks who worked within the executive branch of Government?

Ms. SEYMOUR. Sir, this is an ongoing investigation, and as we uncover new information we are happy to share it with you.

Mr. MULVANEY. Right.

Ms. SEYMOUR. We are not necessarily restricted to the executive branch because there are people who work in the executive branch today who worked in the legislative branch——

Mr. MULVANEY. And I got that notice, Ms. Seymour. I got the notice and it says if you work in the executive branch or you have ever worked in the executive branch, then there is a chance they got your data, but if you have never worked for the executive branch, then you don't have to worry.

Are you still comfortable with that statement?

Ms. SEYMOUR. No, sir. This is an ongoing investigation and we are learning new facts every day.

Mr. MULVANEY. And that is a fair answer. Now, the original number we heard publicly was 4 million. Is it still 4 million? I have heard 14 today a couple times. What is the current estimate of the number of current or previous employees who have been affected?

Ms. SEYMOUR. Approximately 4 million is the number that we are making notifications of today. We continue to investigate, especially in the background investigations incident, so that we can understand that data and begin to make notifications there as well.

Mr. MULVANEY. All right, I have a question. I don't think it has been asked yet. I think it is for Mr. Ozment or whoever else understands the IT systems.

When we used to do this in the private sector, we used to differentiate between someone who had hacked into our system and someone who actually stole something form us, because there are two levels of involvement there.

So I guess my question to you, Mr. Ozment, is have you been able yet to make the distinction between just where the hackers were and they had access and things were exposed, and where possibly they actually downloaded data.

Mr. OZMENT. Thank you, Representative.

That is an important distinction and one that we spend a lot of our investigative time examining. For the personnel records, the approximately 4.2 million records, the incident response team, led by DHS but with interagency partners, has concluded with a high probability that that data was exfiltrated, meaning that it was removed from the network by the adversary who took it. And we are continuing to investigate the information related——

Mr. MULVANEY. Very briefly, Mr. Ozment. I appreciate that. I don't mean to cut you off and I wish we had more time to do that. Let me ask this one question. I heard about the data. I heard Mr. Lynch ask about the Social Security numbers. It sounds like that might have been exfiltrated. Health data. Do we collect health data on our employees?

Ms. Archuleta, if I come to work for you or for the Government, do I give you my health records?

Ms. ARCHULETA. Not your health records, but the information regarding your health carrier is the information that we receive and who you would include in the——

Mr. MULVANEY. Okay, so it is not——

Ms. ARCHULETA. No, not your health——

Mr. MULVANEY. So it is not specific medications, it is not specific conditions.

Ms. ARCHULETA. No.

Mr. MULVANEY. It is just who my health insurance company is.

Ms. ARCHULETA. Exactly.

Mr. MULVANEY. Thank you, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

We now recognize the gentleman from Virginia, Mr. Connolly, for five minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

You know, what is so jarring about this hearing is that sort of in bloodless and bureaucratic language we are talking about the compromise of information of fellow Americans and, from the Federal employee point of view, the most catastrophic compromise of personal information in the history of this Country. Social Security records.

Ms. Archuleta, you mentioned that not health information, but health carrier. That is a roadmap to other information hackers can get.

Security clearances. Security clearances are deeply personal and often involve, do they not, Ms. Seymour, unconfirmed negative information, even rumors. I think so-and-so has a drinking problem. That gets in that report even if it is not confirmed. Is that not correct?

Ms. ARCHULETA. Sir, I am not a Federal investigator and I am not familiar with all of the precise data that is in those.

Mr. CONNOLLY. Well, let me confirm for you. It was a rhetorical question, really. It is correct.

How do we protect our employees? Dr. Ozment, when I heard your testimony, it almost sounded like you were saying is that the good news here is we detected the hack. But the object here isn't effective detection, though that is part of the process; it is prevention and preemption to protect our citizens, including Federal employees.

You talked about EINSTEIN and you championed its merits. Was EINSTEIN in place at OPM when this hack occurred?

Mr. OZMENT. Sir, I share your deep concern about the loss of this information and agree that that is a terrible outcome.

Mr. CONNOLLY. A terrible outcome?

Mr. OZMENT. Absolutely. As a Federal employee whose information is itself a part of this database, I feel——

Mr. CONNOLLY. It might even be personally devastating, Dr. Ozment, not just a terrible outcome.

Mr. OZMENT. That is correct, sir.

What I would tell you on this is that EINSTEIN was critical in this incident. As OPM implemented their new security measures and detected the breach——

Mr. CONNOLLY. Was EINSTEIN in place at the time of this breach?

Mr. OZMENT. EINSTEIN 1 and 2 have been in place at OPM. EINSTEIN 3 is not yet available for OPM.

Mr. CONNOLLY. Okay, I only have two minutes. I want to understand your answer. So did it successfully detect a breach had occurred?

Mr. OZMENT. It did not detect the breach that OPM caught on their own networks, because just as the cyber threat information sharing legislation we are focused on acknowledges, you first have to have the threat information. EINSTEIN 1, once we had that threat information, we used EINSTEIN 1 and 2 to detect a separate breach that we were then able to work.

Mr. CONNOLLY. I am sure every Federal employee who had his or her information compromised is comforted by your answer, Dr. Ozment.

Ms. Archuleta, what was the time gap between discovering there had been a breach and the actual breach itself?

Ms. ARCHULETA. We discovered the breach in April of 2015.

Mr. CONNOLLY. This year. And when did t he breach occur?

Ms. ARCHULETA. We suspected it happened earlier in 2014.

Mr. CONNOLLY. So some time late last year?

Ms. ARCHULETA. Yes, sir.

Mr. CONNOLLY. Okay. So whoever were the hackers, presumably an agency of the Chinese government, according to published reports confirmed by U.S. officials, it is not a classified piece of information. The details of it may be, but our Government, I believe, has confirmed, without attribution, in public records that it was a systematic effort by the People's Liberation Army, which has been notorious for hacking all over the West, that got its hands on this data.

So they had four months in which to do something with this data, is that correct, maybe five?

Ms. ARCHULETA. I can't make a comment on attribution.

Mr. CONNOLLY. I didn't ask you to. I just asked whether they had four or five months to do something with this data.

Ms. ARCHULETA. The period between when we believe the breach occurred and our discovery, yes.

Mr. CONNOLLY. All right.

I am going to, real quickly, if the chairman allows, ask Mr. Scott one last question. The head of CERT, the director of CERT says if the agency implemented three steps, we could prevent about 85 percent of breaches.

And I am going to hold in abeyance new investments and new technology because Ms. Seymour talks about legacy systems, and I had always hoped that the Chinese didn't know how to hack into COBOL. But that is a different matter.

Okay, the three things are minimize administrator privileges; two, utilize application whitelisting; and, three, continuously patch software, which, interestingly, does not go on.

Would you just comment? What is your professional take on those three recommendations?

Mr. SCOTT. I think those recommendations are great, and there are a number of other things as well, some of which I have talked about today. I think the one point I would make is there is no one measure that you could say that is going to prevent all attacks or

even prevent an attack. It is really defense in depth is your best measure, and that is what we are really looking at emphasizing.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank you.

We now recognize the gentleman from North Carolina, Mr. Walker, for five minutes.

Mr. WALKER. Thank you, Mr. Chairman.

I certainly agree with my colleague from Virginia in his description this is a catastrophic compromise.

Ms. Archuleta, it appears that OPM did not follow the very basic cybersecurity best practices, specifically such as network segmentation and encryption of sensitive data. Should the data have been encrypted? Can you address that?

Ms. ARCHULETA. At that time, the data was not encrypted, and as Dr. Ozment has indicated, encryption may not have been a valuable tool in this particular breach. As I said earlier, we are working closely to determine what sorts of additional tools we can put into our system to prevent further breaches.

Mr. WALKER. You said may not have been. But that didn't answer the question should have been encrypted and could that have been another line of defense?

Ms. ARCHULETA. I would turn to my colleagues from DHS to determine the use of encryption, but I will say that it was not encrypted at the time of the breach.

Mr. OZMENT. I would note that if an adversary has the credentials of a user on the network, then they can access data even if it is encrypted, just as the users on the network have to access data, and that did occur in this case, so encryption in this instance would not have protected this data.

Mr. WALKER. I want to delve a little further in just a moment, but let me ask this.

Ms. Archuleta, what consequences should CIO's face for failing to meet such a baseline of cybersecurity standard on their networks? May I hear your thoughts on that?

Ms. ARCHULETA. I believe that the CIO is responsible for the implementation of a solid plan and I believe that my CIO has been doing that. We are working with a legacy system that is decades old, and we are using all of our financial and human resources to improve that system. Cybersecurity is a government-wide effort and we all must work together to improve the systems that we have government-wide.

Mr. WALKER. I am not sure that the American people are content with the pace of how we are all working together.

I want to speak a little bit to EINSTEIN. I have heard several different comments today regarding it and my question is even if EINSTEIN is a necessary component to effectively defending the system, I believe the private sector is really already moving on this kind of technology. Is that a fair question? And what is the DHS doing to keep pace with its attackers? Dr. Ozment?

Mr. OZMENT. EINSTEIN is absolutely a necessary, but not sufficient, tool for protecting department and agency networks. As Mr. Scott has noted several times, we need a defense in depth strategy. We are supplementing EINSTEIN with continuous diagnostics and mitigations at the agencies, and we are also looking with EIN-

STEIN at taking what is currently a signature focus system and adding capabilities to let it detect previously unknown intrusions.

But as you do that you also receive more false positives. In other words, you receive more indications that an intrusion occurred even if it did not occur. So we have to do that carefully so we are not overwhelmed by essentially bad data.

Mr. WALKER. And it seems to be that you are more excited or more confident in the EINSTEIN, what is it, 3A version? Is that going to be more solid as far as keeping the attackers out?

Mr. OZMENT. EINSTEIN 3A will be a step forward. It uses classified information and is modeled on a similar Department of Defense program. It is still a signature-based program, but it will rely upon classified information obtained from the intelligence community to help us detect adversaries and block them.

Mr. WALKER. And I even heard you earlier say something about how even that system needs to be supplemented with others, is that correct?

Mr. OZMENT. That is correct. Again, no single system here will solve this problem.

Mr. WALKER. And there lies my problem, because even on the DHS's own Web site, when talking about EINSTEIN 3, it says it "prevents malicious traffic from harming networks."

Now, if that is not all-inclusive, should not we be understanding that before today's hearing? Why are we just now getting this information that this may not be enough to prevent such, as we said earlier, catastrophic compromise?

Mr. OZMENT. I can't speak to the web page you are referring to, but I can say that we have been very consistent and I have been very consistent in all my interactions with Congress to highlight that we do need to a defense-in-depth strategy and that no one tool will solve all of our problems.

Mr. WALKER. And who is responsible for posting this information on the Web site of the DHS?

Mr. OZMENT. We will look into that and get back to you, sir, and make updates as necessary.

Mr. WALKER. Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. Thank you.

Now recognize the gentleman from Pennsylvania, Mr. Cartwright, for five minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman.

I thank the chairman and the ranking member for calling this hearing.

Director Archuleta, I know there have been much bigger data breaches than this one, but I am concerned, and I share the sentiments of Mr. Connolly from Virginia. This is extremely troubling. We are talking about 4 million-plus Federal workers, people who dedicate their entire careers, indeed, their entire lives, to our Country, and now their personal information has been compromised through absolutely no fault of their own.

If I understand your testimony, the personal information of about 4 million current and former employees was potentially compromised, and I want to ask you, as your investigation continues, do you believe that that number is going to be bigger than 4 million?

Ms. ARCHULETA. Thank you for your question. In my opening statement I described two incidences.

Mr. CARTWRIGHT. No, it is a yes or no question, or I don't know.

Ms. ARCHULETA. No. Because of the two incidents, the first incident is 4.2 million, and an ongoing investigation led us to understand that the Federal investigative background checks——

Mr. CARTWRIGHT. You know what I mean when I say it is a yes or no question, right?

Ms. ARCHULETA. Yes, sir.

Mr. CARTWRIGHT. Okay. Do you think it could be more than 4.2 million?

Ms. ARCHULETA. Yes, sir.

Mr. CARTWRIGHT. Okay.

Now, Ms. Seymour, let me turn to you for some more detailed responses.

Your IT professionals discovered the breach in April and also, as Mr. Connolly mentioned, they believe the hack may have begun back in December, am I correct in that?

Ms. SEYMOUR. Yes, sir, it began in 2014.

Mr. CARTWRIGHT. Now, something else happened in December of 2014; OPM's contractor, Keypoint, revealed that it was targeted in an earlier cyber attack. Now, this is the contractor that does the majority of your agency's background check investigations, am I correct in that?

Ms. SEYMOUR. They do a number of our background investigations, sir. I am not sure of the numbers.

Mr. CARTWRIGHT. And in that case the attack against Keypoint was successful; personal information was, in fact, compromised, correct?

Ms. SEYMOUR. Yes, sir.

Mr. CARTWRIGHT. On Friday, ABC News issued a report entitled "Feds Eye Link to Private Contractor in Massive Government Hack." This article says this, "The hackers who recently launched a massive cyber attack on the U.S. Government, exposing sensitive information of millions of Federal workers and millions of others, may have used information stolen from a private government contractor to break in to Federal systems." The article goes on, "The hackers entered the U.S. Office of Personnel Management, OPM's computer systems after first gaining access last year to the systems of Keypoint Government Solutions."

It continues, "Authorities, meanwhile, believe hackers were able to extract electronic credentials or other information from within Keypoint systems and somehow use them to help unlock OPM systems, according to sources. The hackers then rummaged through separate segments of OPM systems, potentially compromising personal information of not only the 4 million current and former Federal employees."

Ms. Seymour, I know we are having our classified briefing later, and I thank you for coming to that, but can you comment on these reports? Did these hackers actually get what they wanted in the previous attack against OPM's contractor, Keypoint, so they could then go after OPM itself?

Ms. SEYMOUR. I believe that is a discussion that we should have in a classified setting, sir.

Mr. CARTWRIGHT. Fair enough.

Now, we know that OPM's other contractor, USIS, was also breached last year and that its information was also compromised. Can you tell us if those hackers got information in the USIS breach that they were then able to use in the attack against OPM?

Ms. SEYMOUR. Again, that is a discussion we should have later, sir.

Mr. CARTWRIGHT. I understand. I certainly don't want you to disclose classified information here.

Let me close by asking a final question to the whole panel, and I will let each of you answer. Federal agencies and private companies are only as strong as their weakest link. Last year we saw breaches of two contractors, Keypoint and USIS. Now we have reports that these hackers are getting into OPM information because of what they learned in those hacks.

Agencies have leverage over their contractors using the provisions in the contracts and the billions of taxpayer dollars that they pay out to the company, so I want to ask each of you how can agencies use that leverage to improve cybersecurity practices of contractors so that they do a better job of safeguarding the information that they are entrusted with.

Go ahead, right on down the line, starting with you, Ms. Archuleta.

Ms. ARCHULETA. What we can do with the contractors that we engage is to make sure that they have the security systems that match the Federal Government's and that they are using the same sort of types of systems.

I want to be sure that I understand your question. The contractors that we employ as individuals or as companies

Mr. CARTWRIGHT. The contractors as companies.

Ms. ARCHULETA. In our contracts with the companies, we are now working to make sure that they are adhering to the same standards that we have in Federal Government, as outlined in our rules.

Mr. CARTWRIGHT. Dr. Ozment?

Mr. OZMENT. Representative, DHS, for its own contract, as one example, has been working to build in additional cybersecurity requirements. I would also point you to the FedRAMP effort, government-wide effort to establish a baseline of cybersecurity requirements for cloud contractors to the Government.

Mr. CARTWRIGHT. Mr. Scott?

Mr. SCOTT. Yes. I think as my colleague, Anne Rung, and I testified last week, we also are strengthening the Federal contract procurement language and creating contract language that any agency can use as a part of their standard contracts.

Mr. CARTWRIGHT. Thank you.

Ms. Burns?

Ms. BURNS. I think it is about beefing up the security clauses in all contracts so that they cover the full extent of what we need, and then doing the monitoring and follow-up that you need to do to ensure that the contractors are adhering to those clauses of the contract.

Mr. CARTWRIGHT. Right.

Ms. Seymour?

Ms. SEYMOUR. I agree with everything that my colleagues have put forth, but I will add that site inspections are also important, and those are some of the things that we do at OPM with our contractors, as well as continuous monitoring. Looking at a system every third year is not ample. That is not a best practice and we need to move more towards looking at different security controls at different intervals of time.

The other option that we do use is our IG also does inspections of our contractor companies.

Mr. CARTWRIGHT. Mr. Esser?

Mr. ESSER. I agree with what the other witnesses stated. Like Ms. Seymour just said, we, as the IG, go out and we do audits of contractors, health insurance companies, the background investigation companies, as well. So we can be used and see ourselves in that role.

Mr. CARTWRIGHT. Mr. Chairman, I thank you for your indulgence. I also want to note that USIS was invited here today, but refused——

Chairman CHAFFETZ. I appreciate the gentleman. You are almost three minutes over time. We have classified that we have to go to and we have members that still have an effort.

Mr. CARTWRIGHT. Yield back.

Chairman CHAFFETZ. Thank you. Appreciate it.

I now recognize Mr. Russell from Oklahoma for five minutes.

Mr. RUSSELL. Thank you, Mr. Chairman.

I am baffled by all of this. Upon receipt or upon your appointment of the directorship of OPM, Director Archuleta had stated that she was committed to building an inclusive workforce. Who would have thought that that would have included our enemies.

In this testimony here today, we heard statements that we did not encrypt because we thought they might be able to decrypt or decipher. That is just baffling to me.

There was another statement I heard earlier today that said had we not established the systems, we would never have known about the breach. That is tantamount to saying if we had not watered our flower beds, we would have never seen the muddy footprints on the open windowsill.

I mean, this is absolute negligence that puts the lives of Americans at risk, and also foreign nationals that interact with these Americans. Of particular concern are the SF 86 forms, of which I am very familiar, with my background prior to coming to Congress.

We had Sean Gallagher from Ars Technica, who summed it up probably best. He said that this breach was a result of inertia, a lack of internal expertise, and a decade of neglect.

Director Archuleta, why did you not shut down 11 of the 21 systems that had no security assessment and authorization?

Ms. ARCHULETA. Sir, as I mentioned before, there are numerous priorities that go into employee safety and security, including making sure that our retirees receive their benefits or that our employees get paid. There are numerous considerations that we had to——

Mr. RUSSELL. Would one of those considerations be encrypting Social Security numbers? I mean, does it take a degree in IT in cybersecurity to encrypt Social Security numbers? I didn't think so.

Did your cybersecurity strategic plan including leaving half of OPM's systems without protection when you formulated it? Was that part of the plan?

Ms. ARCHULETA. No, sir.

Mr. RUSSELL. Then why was it not made a priority?

Ms. ARCHULETA. The systems that the IG referred to in our plan, those systems that he recommended that we shut down, he recommended that we shut them down because they were without authorization. All of our systems are now authorized and they are operating.

I have to say that we are looking at systems that are very, very old, and we can take a look at encryption and other steps that could be taken, and certainly we are doing that, but as we look at this system, we are also having to deal with decades of——

Mr. RUSSELL. Well, I understand that, but I also understand there is an old saying we had in the military: poor is the workman who blames his tools. Missions can be accomplished even with what you have, and measures could have been done had this been made a priority. What I see now is why did OPM have no multi-factor authentication for users accessing the system from outside OPM? There was no multi-faceted means. If they get into the system, they have free rein, is that correct?

Ms. ARCHULETA. We have implemented multiple factors. Ms. Seymour has mentioned multi-factor authentication with our remote users and are working now.

Mr. RUSSELL. And when was that put in place, before or after the breach?

Ms. ARCHULETA. This began in January of 2015.

Mr. RUSSELL. Okay. So stolen credentials could still be used to run free in the system, is that correct?

Ms. ARCHULETA. Prior to the time of the two-factor authentication, obviously, it takes time to implement all of these tools. I am as distressed as you are about how long these systems have gone neglected when they have needed much resources, and it is in my administration that we have put those resources to it. We have to act quickly, which we are doing, and we are also working with our partners across government.

As I said before, cybersecurity is an issue that all of us need to address across the Federal Government.

Mr. RUSSELL. Was a priority made to these outside systems that were most vulnerable that would allow this type of free run?

Ms. ARCHULETA. I am sorry, sir, would you repeat the question?

Mr. RUSSELL. Was a priority made to these outside accessing systems to OPM's database that once they get in them they have a free rein, a free run?

Ms. ARCHULETA. Yes, it was a priority, sir, but as I said before, legacy system, it takes time.

Mr. RUSSELL. It didn't take our enemies time.

Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

Now recognize the gentleman from California, Mr. Lieu, for five minutes.

Mr. LIEU. Thank you, Mr. Chairman.

Director Archuleta, under your watch, last March, OPM database containing the crown jewels of American intelligence was breached. This year the same exact database was breached. A third database containing over 4 million Federal employees' data unencrypted was breached.

The IG has said that at OPM your technology systems are either materially weak or seriously deficient, and my question to you, just a very simple yes or no, is do you accept responsibility for what happened?

Ms. ARCHULETA. I accept responsibility for the administration of OPM and the important role of our IT systems in delivering the services, and I take very seriously my responsibilities in overseeing the improvements to a decades-old legacy system.

Mr. LIEU. I don't really quite know what that means. I asked for a yes or no. But that is fine, you have answered it.

I am going to reserve the balance of my time to make a statement. Having been a member of this oversight committee, and as a computer science major, it is clear to me there is a high level of technological incompetence across many of our Federal agencies. We have held hearings where it showed that Federal agencies couldn't procure, implement or deploy IT systems without massive bugs or massive cost overruns.

We have held hearings where at least one Federal agency, in this case the FBI, had a fundamental misunderstanding of technology, where they continue to believe they can put in back doors to encryption systems just for the good guys and not for hackers, which you cannot do. We had over 10 federal data system breaches last year.

So there is a culture problem and there is a problem of civilian leadership not understanding we are in a cyber war. Every day we are getting attacked in both the public and private sector. The U.S. military understands this; that is why they stood up an entire cyber command. But until our civilian leadership understands the gravity of this issue, we are going to continue having more data breaches.

Let me give you some examples of this culture problem. You have heard today there was unencrypted Social Security numbers. That is just not acceptable. That is a failure of leadership.

Look at the various IG reports over the years showing material weaknesses and then look at last year's IG report, page 12, that says as of November of last year, OPM had not yet done a risk assessment. That is ridiculous, especially since you knew in March your system was breached. That is a failure of leadership. And this goes beyond just OPM.

Now, Mr. Scott, you have only been here a few months, so you are going to get a pass on this, but I want to know why was it that it wasn't until last Friday that agencies were ordered to put in basic cybersecurity measures? Why wasn't this done last year? Why wasn't this done years before? There is a failure of leadership above that of OPM.

And when there is a culture problem, what have we done in the past? Especially in the area of national security, you can't have the view that, oh, this is legacy system, oh, we have these excuses. In

national security it has to be zero tolerance. That has to be your attitude. We can't have these breaches.

The CIA can't go around saying, you know, every now and then our database of spies is going to get breached. That cannot happen.

And when you have a culture problem, as we have hard here, in the past, when agencies have had this, leadership resigns or they are fired. At the DEA, leadership left. We had this happen at the Secret Service; we had this happen at the Veterans Administration. And we, as a government, do that for two reasons: one is to send the signal that the status quo is not acceptable. We cannot continue to have this attitude, where we make excuse after excuse.

You know, I have heard a lot of testimony today. The one word I haven't heard is the word sorry. When is OPM going to apologize to over 4 million Federal employees that just had their personal data compromised? When is OPM going to apologize to the Federal employees that had personally devastating information released through the SF 86 forms? I haven't heard that yet.

And when there is a culture problem, we send a signal to others that the status quo is unacceptable and leadership has to resign. Another reason we do that is because we want new leadership in that is more competent.

So I am looking here today for a few good people to step forward, accept responsibility, and resign for the good of the Nation. I yield back.

Chairman CHAFFETZ. I thank the gentleman. Well said.

Now recognize the chairman of the IT subcommittee, Mr. Hurd, of Texas, for five minutes.

Mr. HURD. Thank you, Mr. Chairman.

It is my hope that every agency head and every CIO of these agencies are listening or watching or will read the testimony after this event, and that the first thing they do when they wake up tomorrow is pull out the GAO high risk report that identifies areas that they have problems with, they read their own IG report and start working to address those remediations.

I have been at this job for 21 weeks, similar to Mr. Scott, and one of the things you hear from people, they are frustrated with their Government. Intentions are great.

Ms. Archuleta, you said at the beginning that the security of Federal employee is paramount. I believe you believe that, but the execution has been horrific. Intentions are not enough. We have to have execution. And this is the thing that scares me.

So my question, let's start with you, Ms. Archuleta. Did the hackers use a zero day vulnerability to get into your network?

Ms. ARCHULETA. I think that would be better answered in a classified setting.

Mr. HURD. Well, if it was a zero day vulnerability, I hope everybody has been notified of this zero day; not only the Government, but the private sector. We shouldn't be keeping secret a zero day vulnerability.

I know a little something about protecting secrets; I spent almost my adult life in the CIA doing that. This is something that we need to get out. What I have read is that EINSTEIN did detect the breach after the appropriate indicators of compromise was loaded into it.

So my question is how long did, in Federal Government, did somebody have access to these indicators of compromise and why did it take however much that time to get it into EINSTEIN's system, and has that been promoted to every other agency that is using EINSTEIN 2?

Mr. OZMENT. Representative, OPM, once they implemented their security measure and discovered this breach, gave us the indicators of compromise immediately and we loaded it into EINSTEIN immediately. That is, we loaded it into EINSTEIN 2 to both detect and we looked back through history to see if any other traffic back in time had indicated a similar compromise. That is how we found an intrusion into OPM related to this incident that led to our discovery of the breach of the personal records.

We also put it into EINSTEIN 3 so that agencies covered by EINSTEIN 3 would be protected against a similar activity moving forward. And then we held a call with all the Federal CIOs and disseminated these indicators to them and asked them to search their networks for these indicators.

Mr. HURD. Has that been done?

Mr. OZMENT. That has been done.

Mr. HURD. Okay.

Ms. Seymour, you talk about legacy systems and the difficulty of protecting those. What are some of those legacy systems and what programming software is used to develop those systems?

Ms. SEYMOUR. These are systems, sir, that have been around for going close to 25, 30 years.

Mr. HURD. So it was written by COBOL?

Ms. SEYMOUR. COBOL systems. One of the things I would like to offer is that Director Archuleta and I actually were brought here to solve some of these problems.

Mr. HURD. When did you start your job?

Ms. SEYMOUR. In December of 2013.

Mr. HURD. And why did we wait to implement two-factor authentication until after the attack?

Ms. SEYMOUR. We have not waited, sir.

Mr. HURD. So two-factor authentication was being deployed prior?

Ms. SEYMOUR. These are two decades in the making. We are not going to solve them all in two years. And if we continue——

Mr. HURD. See, what is where I disagree with you, okay? Again, we have to stop thinking about this that we have years to solve the problem. We don't. We should be thinking about this in days.

Ms. Archuleta, how much overtime have you signed off on since this hack, of people that are dealing with the compromise?

Ms. ARCHULETA. My CIO team works 24/7.

Mr. HURD. So if I walk into your building at 8 p.m. at night, there are going to be people drinking Red Bull, working furiously in order to solve this problem?

Ms. ARCHULETA. I am very proud of the employees that are working on this issue, and they have been working 24/7.

Mr. HURD. Mr. Scott, you have inherited a mess, my man, and we are looking to you, and whatever this committee can do to help you to ensure things like this doesn't happen, to ensure that these agencies and the CIOs of the agencies are implementing the rec-

ommendations of the IG, the recommendations of the GAO, we are here to do that. And we are going to continue to drag people up here and answer these questions, because that is our responsibility.

I recognize that you are not going to stop anybody from penetrating your network. But how quickly can you identify them, can you quarantine them, and can you kick them off the network? Those are the three metrics we should be using about the health of our systems, and we are woefully inadequate.

I yield back the time I do not have. Thank you, sir.

Chairman CHAFFETZ. Thanks.

Mr. DeSantis, of Florida, is now recognized for five minutes.

Mr. DESANTIS. Thank you, Mr. Chairman.

Ms. Archuleta, in your testimony you said, and I think this is the direct quote, "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 was not stored on OPM's system."

What do you mean by service history?

Ms. ARCHULETA. Their careers. They may have been in a different position earlier than perhaps as they move around Government, so it may be someone whose current job would not be in the system, but because of their service history their information would be dated back, and it is for retirement purposes.

Mr. DESANTIS. Okay, so a potentially broader breach.

I tell you, an SF 86, I remember filling that out when I was a young officer in the Navy, and it is by far the most intrusive form that I have ever filled out. It took me days. I had to go do research on myself to try to figure out. And it is not just that you are doing a lot of personal and sensitive data about the individual applicant, the SF 86 asks about family members, it asks about friends, spouse, relatives, where you have lived, who you knew when you lived in these different places. It also asks you to come clean about anything in your past life.

So, to me, people have said that this is crown jewels material in terms of potential blackmail. So this is a very, very serious breach.

My question for Ms. Archuleta, were cabinet level officials implicated in this breach?

Ms. ARCHULETA. Sir, this type of information would be better discussed in a classified setting.

Mr. DESANTIS. Understood. What about people in the military and intelligence communities?

Ms. ARCHULETA. As I mentioned earlier, I believe that this is something that we could respond to in a classified setting.

Mr. DESANTIS. Okay. So you don't disagree with my characterization of the SF 86 and that the compromise, let's just say theoretical if you don't want to say what actually happened here, that that is a major, major breach that will have ramifications for our Country?

Ms. ARCHULETA. As I said, we will discuss this with you in the classified setting.

Mr. DESANTIS. Okay. SF 86 forms also require applicants to list foreign nationals with whom they are in close contact, so that means China now has a list, for example, of Chinese citizens world-

wide who are in close contact with American officials. They can, and will, obviously us that information for espionage purposes.

So what are the security implications of that type of information falling into enemy hands? That could be for anybody.

Mr. OZMENT. Sir, that is a question that we will discuss in the hearing this afternoon.

Mr. DESANTIS. Okay. Now, some reports say that not only were the hackers pursuing information on Federal employees, but also password and encryption keys that could be used for trade secret theft and espionage. And I guess you will have more to say about that in a classified setting, but at least for this forum can you say that that is a significant risk; that is not the type of information that we would want the enemy to have and it can, in fact, be very damaging, correct?

Mr. OZMENT. Again, sir, we are going to defer discussion on that until the classified briefing in a few minutes.

Mr. DESANTIS. Okay. And I get that and I will be there and I will listen intently. But it really concerns me because this is really a treasure trove for our enemies, potentially. And the fact that this system was hacked and we didn't even know about it for a long time, that is really, really troubling.

If you ask people if they want to serve in these sensitive positions and they think that by filling out these forms they are actually going to put themselves or their family potentially at risk because the Government is not competent enough to maintain that secretly, that is a major problem as well. So the information can be used against the Country, then you are also, I think, going to have a chilling effect on people wanting to get involved if we don't get a handle on this.

So I look forward to hearing from the witnesses in a classified setting and I yield back the balance of my time.

Chairman CHAFFETZ. Thank you.

Now recognize the gentleman from Alabama, Mr. Palmer, for five minutes.

Mr. PALMER. Thank you, Mr. Chairman.

Ms. Seymour, does the employee exposure extend only to those who filled out Standard Form 86, or does it include others as well?

Ms. SEYMOUR. Our investigation is ongoing, sir.

Mr. PALMER. Well, ma'am, apparently it does, because I have two employees who have never filled out a Standard Form 86, and they have a letter from you informing them of the possibility that their data may have been compromised. So I will ask you again, and it is a yes or no, does it extend beyond the people who filled out an SF 86?

Ms. SEYMOUR. My answer to that is yes, sir. There are two incidents that we have come here to talk with you today.

Mr. PALMER. Why didn't you answer yes to start with?

Ms. SEYMOUR. Because you were talking about SF 86s, sir.

Mr. PALMER. No. I made it clear. I asked you, did the exposure extend beyond those who filled out SF 86, and you said the investigation was ongoing. Apparently, you have investigated enough to send a letter to employees who didn't fill out those forms, so thank you for your yes answer.

In your judgment, Ms. Archuleta, how likely is it that the hackers were able to access these personnel files through an employee account?

Ms. ARCHULETA. Sir, we will be able to discuss that with you during the classified session.

Mr. PALMER. Well, let me be a little bit more specific. Are you familiar with The Wall Street Journal article that indicated that it was possible that the breach occurred through personal email accounts, because employees were using the Federal system and that early in 2011 the Immigration and Customs Enforcement agency noticed a significant up-tick in infections and privacy spills, and they asked for a directive or they put out a directive that Federal employees could not use the Federal system to access their personal emails? But the American Federation of Government Employees filed a grievance with the federal arbitrator claiming that that was something that needed to be bargained and needed to be part of the collective bargaining agreement.

The arbitrator dismissed ICE's security arguments in 75 words, claiming that the law didn't give the Federal agencies exclusive discretion to manage the IT systems, so ICE wasn't able to shut that off. Do you have any comment on that?

Ms. ARCHULETA. No, sir. Again, those are issues that we will be able to discuss in the classified hearing.

Mr. PALMER. Well, it is being discussed in The Wall Street Journal.

I think for now, since we need to head to the hearing, I will yield the balance of my time.

Thank you, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

Now recognize the gentleman from Georgia, Mr. Hice, for five minutes.

Mr. HICE. Thank you, Mr. Chairman.

Mr. Esser, what are the risks that are associated with not having a valid system authorization?

Mr. ESSER. Well, the risks are evident that not having a valid authorization essentially could be a symptom of weak controls over operating systems and applications, and lead to things such as a breach.

Mr. HICE. Okay. With all the things that we are talking about here today, Ms. Seymour, you were obviously fully aware of these risks and OPM was aware of these risk?

Ms. SEYMOUR. Yes, sir, I was aware of these reports.

Mr. HICE. Okay.

Now, I kind of hate going back to this because it has come up several times already today, but still I am waiting for an answer. The inspector general put out his report last November expressing great alarm, recommending that OPM consider shutting down the systems because of the risks that you knew about, Ms. Archuleta knew about, and yet these recommendations were ignored.

Now, I am going to come back to you with this because, quite frankly, Ms. Archuleta has tried to dodge this question and dance all around it. I want to come straight up with you. Why were those recommendations not followed?

Ms. SEYMOUR. Two reasons, sir. One is an authorization to operate is merely the documentation of the security controls of a system and their effectiveness. That does not mean simply because you don't have an authorization that those tools don't exist.

The other effort is, as the IG was doing its audit, we were taking all of those vulnerabilities into play. We had already developed a security plan that we were in the process of implementing, and the IG admits in their report that we were in the process of implementing many of those controls.

Mr. HICE. Did the plan that you were in process of implementing work? Obviously, it didn't. Would shutting it down have worked?

Ms. SEYMOUR. The controls that we put in place allowed us to stop the remote access to our network, and they also allowed us to detect this activity that had occurred prior to the IG report.

Mr. HICE. But the vulnerability was still there and your plan failed.

Ms. SEYMOUR. There are vulnerabilities in every system. What we do is a risk management process, sir, where we look at the vulnerabilities as well as the business that we must conduct.

Mr. HICE. Mr. Esser, let me come back to you. Currently, what are the consequences of owners of OPM IT system? Currently, what are the consequences now if they operate without a valid authorization?

Mr. ESSER. There are essentially no consequences. We report that in our FISMA audits, but other than that there are no official sanctions in place. It is something that gets publicized, and that is the extent.

Mr. HICE. So it sounds to me like this thing is still not being taken seriously. If there are no consequences for operating without authorization, why in the world are we still operating without authorization? Or is that occurring?

Ms. SEYMOUR. Sir, I have extended the authorizations that we had on these systems. Because we put a number of security controls in place in the environment, we have increased the effectiveness of the security around those systems.

Mr. HICE. But there are no consequences for not operating on a system with authorization, so how seriously are you taking it?

Ms. SEYMOUR. There are consequences.

Mr. HICE. What are they?

Ms. SEYMOUR. Those consequences are if you aren't doing the assessments, documenting them, while that is evidence that those assessments have been done, the assessments themselves are more important; the scanning of the network, the tools that are in place.

Mr. HICE. That is not the consequences. What are the consequences? You said there are consequences. I want to know what they are.

Ms. SEYMOUR. The consequences that we have are we report to OMB on a quarterly basis about the status of our security and our network.

Mr. HICE. That doesn't sound like consequences; that sounds like just reporting that you are required to do anyway. There are no consequences involved in those reports.

Mr. Esser, again, are there measures that need to be taken to get the whole thing up to the standard it ought to be? I mean, is there anything that you would recommend?

Mr. ESSER. Yes. Yes. We do recommend that the CIO, the agency take the steps that in a lot of cases they are beginning to take. The centralization of the IT governance is well along the way. What they also need to do is get a full inventory of the assets that they are responsible for protecting.

The shell project that Ms. Seymour has alluded to earlier is also something that we support. We also have some concerns about the way the project has been started and managed, but overall we support the idea behind the shell project.

Chairman CHAFFETZ. We appreciate the gentleman.

We now recognize the gentlewoman from New Mexico, Ms. Lujan Grisham, for five minutes.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman. Thank you for having this important hearing.

I want to thank the panel for taking this conversation and these questions so seriously.

In New Mexico, we are one of the States that has one of the largest percentage or per capita Federal employees in the Country, in the top five, so I have 50,000 Federal employees in my home State, and I am on their side by being incredibly concerned about this and, quite frankly, many other data breaches.

The growing sophistication, frequency, and the impact on both public and private entities by cyber attacks continue to be a very serious threat. In fact, two days after my first election, one of the key briefings by one of the national labs which is in my district on Kirkland Air Force Base is the continuing growing concern with cybersecurity issues and their aggressive responses both to be proactive as much as they can and to appropriately be reactive once you have an identifiable breach.

Given the data breach at OPM and at Home Depot and at Target, Anthem, it is clear to me that not only does the Federal Government have a role in protecting Federal employees and the information that you have, but we have a role in working to protect the public in general from these serious and continuing series of cyber attacks.

But I recognize also that this is a very challenging effort and that there is not a simple solution. If there was, we could stop this hacking altogether and have the magic bullet. And as much as I want you to do that, I don't want to minimize the fact that I recognize that that is more difficult to say than do. No, it is easy to do; it is not so easy to do. But my concerns are growing given that even the best in the Country are facing significant cyber attacks, including Kaspersky Lab, who we are relying on for innovative and appropriate technologies to implement.

So given that diatribe and given all the questions that you have had about accountability, about the serious nature, here is really my question. The Federal Government is not known for being, and I mean no disrespect by this, but just stating the facts, it is not a proactive, very reactive body just by the nature of how large it is, how broad our mission is, and how we are dependent on whatever the resources are and the priorities are at any given time.

Given that climate and the role to protect the general public and your role to protect Federal employee information, what can you do that is different, that puts you in a position to be much more proactive, particularly given the nature of cyber attacks? Quite frankly, they have already hacked in as you are making the next modifications.

Anyone on the panel. Mr. Scott, that may be a question that is primarily for you, but I would be interested in anybody's response.

Mr. SCOTT. Sure. I can think of several things in the short run that actually we already have underway, but probably long-term the biggest thing is to double down on replacing these legacy sort of old systems that we have. One of the central problems here is you have old stuff that just was not designed or built in an era when we had these kinds of threats, and it is, in some cases, very, very hard to sort of duct tape and band aid things around these systems.

It doesn't mean there is nothing you can do, but fundamentally it is old architectures that need to be replaced and security needs to be designed into the very fabric of the architecture of the hardware, the software, the networks, the applications. And the faster we can do that, the faster we are on a better road.

Ms. LUJAN GRISHAM. And given your role to do that in Federal Government, I am not clear today what percentage of legacy systems and old architecture platforms that we are still operating under and which departments are more at risk than others. What is the time frame for getting that done and what is a reasonable course for this committee to take to make sure we have accountability in Federal Government to move forward exactly in that effort?

Mr. SCOTT. Well, I think the first thing is we are going to be very transparent with you in terms of the OMB reports in terms of where we are at on that journey as we go through our work over the course of the year. Several of the members of this committee have said they are going to pay very close attention to that, which I encourage.

Chairman CHAFFETZ. The gentleman will suspend.

Our time is so tight to our 1:00 o'clock briefing. We would like a full and complete answer. There will be questions for the record and we will continue to follow up, and I hope you understand.

Mr. SCOTT. Be happy to.

Chairman CHAFFETZ. We need to give time to Mr. Grothman from Wisconsin, who is now recognized for five minutes.

Mr. GROTHMAN. I am glad we have established that the Federal Government is not a proactive, reactive body. It is something for us to always remember, no matter what bill moves around here. It is something to remember about the Federal Government.

But be that as it may, the first question I have for you guys, this is kind of a significant story here. Just out of curiosity, just to see how the Federal Government operates, has anybody lost their job over this or have there been any recriminations in that regard?

Ms. ARCHULETA. No, sir.

Mr. GROTHMAN. Okay. Next question, I don't care who answers it. As I understand, it took months for the State Department to root out the Russian hackers in their unclassified systems. Now,

apparently the Chinese hackers are known for leaving behind time-delayed malware. Do we know for sure that these people are out of the system by now or could they still be poking around?

Mr. OZMENT. Representative, we have a joint interagency team led by DHS, with participation by the FBI and National Security Agency, who have worked with OPM and the Department of Interior on this incident. They have accessed that they have fully removed the adversary from these networks, but it is extremely difficult to have 100 percent certainty in these cases.

Mr. GROTHMAN. Okay, so it could be, but you think probably out.

Mr. OZMENT. Yes, sir.

Mr. GROTHMAN. Okay. Final question. Apparently there are rumors that people are now selling some of these files. Is this a threat or do we know if it is going on? And if it is going on, are we doing anything to counter that?

Mr. OZMENT. Sir, I think that the impact and such are questions better suited for the classified briefing we are about to have.

Mr. GROTHMAN. Okay. I yield the remainder of my time.

Chairman CHAFFETZ. Thank you.

I want to thank the panelists and everybody that is here. I think you understand, on a bipartisan basis, how seriously we take this situation.

To those Federal employees who are affected, one of the things that should come out is that in the letter, the very end of the letter, if you receive one of these letters, it does note that the Office of Personnel Management is not going to call you. They are not going to contact you to provide additional information. There will be some very bad actors that are going to try to take advantage of this bad situation and exploit it for their own personal gain. They have already done that. They are going to do it again and there are going to be others that are going to try to do that.

To all of our Federal employees, please do not fall victim yet again to somebody who is going to send you an email or make a call and try to prey upon you further. It was noted in the letter. It is worth noting here from the pulpit.

Again, we look forward to the 1:00 classified briefing. We are going to have to hustle.

The committee now stands adjourned. Thank you.

[Whereupon, at 12:50 p.m., the hearing was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

ABC News: Feds Eye Link to Private Contractor in Massive Government Hack

Jun 12, 2015, 6:45 PM ET
By MIKE LEVINE and JACK DATE
Mike Levine More from Mike »
Digital Journalist, Law Enforcement & Homeland Security
Jack Date More from Jack »

The hackers who recently launched a massive cyber-attack on the U.S. government, exposing sensitive information of millions of federal workers and millions of others, may have used information stolen from a private government contractor to break into federal systems, according to sources briefed on the matter.

Authorities suspect the hackers, likely from China, entered the U.S. Office of Personnel Management's computer systems after first gaining access last year to the systems of KeyPoint Government Solutions -- one of the primary providers of background checks for the U.S. government, sources said.

KeyPoint representatives contacted by ABC News declined comment for this story.

Authorities, meanwhile, believe hackers were able to extract electronic credentials or other information from within KeyPoint's systems and somehow use them to help unlock OPM's systems, according to sources.

The hackers then rummaged through separate "segments" of OPM's systems, potentially compromising personal information of not only the 4 million current and former federal employees already acknowledged publicly but also millions more, including relatives, friends and maybe even college roommates, the sources said.

In an unrelated statement today, OPM said authorities have "a high degree of confidence that OPM systems containing information related to the background investigations of current, former, and prospective Federal government employees, and those for whom a federal background investigation was conducted, may have been exfiltrated," as previously reported by ABC News.

The fact that Colorado-based KeyPoint suffered a cyber intrusion was well-publicized late last year. But the scope of the hack may not have been completely understood at the time by even the nation's top cyber officials, sources indicated. Last year's incident has yet to be officially tied to the recent OPM hack.

The KeyPoint incident, mostly affecting employees of the Department of Homeland Security, was first detected in September, and two months ago DHS began notifying federal employees whose personal information "may have been compromised."

The notification was clear about what information was exposed: "[Your] first and last name, social security number, job title, investigation case number, education history, criminal history, and employment history; spouse or cohabitant's name, date of birth, and social security number; the names, addresses, and dates of birth of relatives of the investigation subject; and names and addresses of friends of the investigation subject."

DHS discovered the KeyPoint intrusion only after undertaking a thorough assessment of all such contractors -- a move prompted by the hacking of another federal contractor, according to DHS.

Asked why the government waited seven months to notify potential victims, one U.S. official said it took time for authorities to conclude personal information may have been stolen in the incident.

Nevertheless, KeyPoint put in place "additional safeguards" after the intrusion was detected, and those steps should "prevent future incidents of this nature," according to the government notification.

In addition to the KeyPoint incident, investigators are also looking into whether another previously-known hack into OPM databases in March 2014 may be connected to the most recent breach.

That attack targeted an OPM system maintaining security clearance information. An OPM official, however, recently told lawmakers it didn't expose any personal information.

Nevertheless, officials strongly suspect the cyber-attack came from China -- just like officials believe the most recent intrusion also came from China.

The most recent OPM hack is believed to have been far deeper and potentially more problematic than publicly acknowledged, sources said, with the hackers believed to have been moving in and out of government databases undetected for more than a year.

Much of the compromised data has been stored on OPM systems housed by the Department of the Interior in a Denver-area data center, sources said. And one of the "segments" compromised held forms filled out by federal employees seeking security clearances.

The 127-page forms -- known as SF-86's and used for background investigations -- require applicants to provide personal information not only about themselves but also relatives, friends and "associates" spanning several years. The forms also ask applicants if they have "illegally used a drug or controlled substance," and they require information on financial history and personal relationships.

That type of information, sources said, could be exploited to conduct "social-engineering" operations, potentially using the data to pressure or trick employees into further compromising their agencies.

Also of concern are U.S. employees stationed overseas, including in countries such as China, whose government would covet personal information on relatives and contacts of American officials living in the communist country, according to officials.

"If the SF-86's associated with this hack were, in their entirety, part of the stolen information, then that would mean the potential release of a staggering amount of information, affecting an exponential amount of people," one U.S. official told ABC News on Sunday.

Acting as the government's human resources division, OPM conducts about 90 percent of background investigations for the federal government. Information from SF-86 forms dating back three decades could have been exposed in the cyber-attack, sources said.

It's still unclear exactly what was compromised by the OPM hack, particularly because OPM officials and other authorities still don't have a good handle on how much information was actually stored by OPM in the first place, one U.S. official said.

Nearly 50 government agencies send data to OPM for storage in some form, according to the official.

The intrusion was only noticed after OPM began to upgrade its equipment and systems. As soon as anomalies within the systems were noticed, the Department of Homeland Security and FBI were notified.

Over two weeks, OPM will be sending notifications to the estimated 4 million current and former government employees whose "Personally Identifiable Information" may have been compromised by the hack.

And "since the investigation is ongoing, additional PII exposures may come to light," an OPM official acknowledged Sunday. "In that case, OPM will conduct additional notifications as necessary."

In a statement last week, an FBI spokesman said, "We take all potential threats to public and private sector systems seriously, and will continue to investigate and hold accountable those who pose a threat in cyberspace."

Efforts to reach an OPM spokesman today were unsuccessful.

Colleen M. Kelley

National President

National Treasury Employees Union

Statement for the Record

For

House Committee on Oversight and Government Reform

"Office of Personnel Management: Data Breach"

June 16, 2015

1750 H Street, N.W. • Washington, D.C. 20006 • (202) 572-5500

Chairman Chaffetz, Ranking Member Cummings and distinguished members of the committee, 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 also commend you for holding this hearing and for devoting Committee attention to this extremely urgent issue. 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 4th, and more recently on June 12th, 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 Committee 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 Committee 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[i] (among others) as part of routine background investigations, including detailed financial information and medical history, home addresses and other PII and data for annuitants. Last Friday evening, 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 statement does 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 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 Committee to ensure that the notification plan for all of these affected individuals is made public, and that it is put into action immediately.

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 identify 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 Committee 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 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. Consideration needs to be given to setting up a process that allows individuals, particularly former employees and retirees, to affirmatively verify whether or not they were impacted by these breaches. Additionally, we are not yet clear whether all information has been announced for this breach.

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 OPM to providing both the credit monitoring services and the identity theft protection services for an extended period of time beyond the current eighteen months. Additionally, we ask that OPM and DHS provide, at no cost, affected individuals with the option of setting up credit freezes with the credit reporting companies. 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 health care breaches, carriers provided twenty-four months of protective services to affected enrollees.

I again thank the Committee 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.

---

[1] Questionnaires for Public Trust, Non-Sensitive, and National Security Positions.

Questions for Mr. Tony Scott
U.S. Chief Information Officer
Office of E-Government and Information Technology
U.S. Office of Management and Budget

Questions from Representative Tim Walberg
Committee on Oversight and Government Reform

June 16, 2015 Full Committee Hearing titled: "OPM Data Breach"

It is clear to me that the current model to defend against cyber-attacks is insufficient. Whether it is Home Depot, Sony, Target and now the Office of Personnel and Management, sophisticated criminals are outwitting the defenses in place. Defense in depth has been our primary strategy and it is a well-worn strategy for defending networks and applications. Unfortunately, many of these defenses rely largely on perimeter devices and security controls. Today's attacks target assets deep within an agency's environment, such as under desktops or endpoints, and they typically come over allowed protocols and applications, such as SSL and email. In addition, mobility has blurred the lines of the perimeter and it is no longer sufficient to rely solely on a defense in depth strategy.

I believe that agencies must also look to new commercial practices to supplement current models to include Zero Trust tenets. My understanding is that technology exists that would allow agencies to build virtual networks and security constructs in an agency platform irrespective of the current architecture they have today.

1. Has the Office of Personnel and Management explored this option?

As a former CIO in the private sector, I am very familiar with current products that allow for micro segmentation of systems and virtualization of servers to allow for hybrid cloud structures which enhance security. These technologies, along with several other existing and emerging technologies, have been identified through the Cybersecurity Sprint efforts as tools that agencies can purchase to broaden their defense in depth strategy. We are working closely with agencies to identify and utilize the latest Commercial Off-the-Shelf (COTS) technologies.

2. If we can use new strategies on our older software why is there a delay in implementing this strategy?

Unfortunately, in a constrained budget environment, agencies are spending close to 80 percent of their total IT budgets on O&M and upkeep of old systems. Implementation of new strategies requires in-depth planning and hardware purchases to allow the reconfiguration of current systems to include modern methods of securing environments. Without additional funds identified or allotted, the deployment of new architecture demands regular technology refreshes and the ability to plan for end-of-life system updates. We value our partnership with Congress and look forward to working with you and your colleagues to ensure a regular, dependable IT budget to allow for modernization of our agencies technology landscape.

3. As we embark on a 30 day sprint to update our networks, is this strategy being discussed? If not, why?

On October 30, 2015, OMB released M-16-04, the Cybersecurity Strategy and Implementation Plan (CSIP). This memo outlines steps that the Federal government is taking to acquire and deploy existing and emerging technology to keep up with changes in the way our government supports our citizens. This is part of the broader Administration effort outlined by the President in the Cybersecurity National Action Plan. This plan directs the Federal Government to take new action now and fosters the conditions required for long-term improvements in our approach to cybersecurity across the Federal Government, the private sector, and our personal lives.