OPM DATA BREACH: PART II

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 24, 2015

Serial No. 114–81

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

22–363 PDF WASHINGTON : 2017

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

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

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

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: PART II

Wednesday, June 24, 2015

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

The committee met, pursuant to call, at 10:03 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Turner, Duncan, Jordan, Walberg, Amash, Gosar, DesJarlais, Gowdy, Farenthold, Massie, Meadows, DeSantis, Mulvaney, Walker, Blum, Hice, Carter, Grothman, Hurd, Palmer, Cummings, Maloney, Norton, Clay, Lynch, Connolly, Cartwright, Duckworth, Kelly, Lawrence, Lieu, Watson Coleman, Plaskett, DeSaulnier, Welch, and Lujan Grisham.

Also Present: Representative Comstock.

Chairman CHAFFETZ. Good morning. The Oversight Committee is coming to order. Our hearing today is about the OPM data breaches. This is part 2.

$529 billion: $529 billion is how much the Federal Government has spent on IT since 2008. Roughly $577 million has been spent at the Office of Personnel Management. Roughly 80 percent of that money has been spent on legacy systems, and we're in a situation here where the hurricane has come and gone, and just now OPM is wanting to board up the windows. That's what it feels like.

This is a major, major security breach, one of the biggest—if not the biggest—we have ever seen. This demands all of our attention and great concern about what happened, how we're going to prevent it from happening in the future, and what are we going to do with the information now? Because there is no simple, easy solution, but I can tell you, oftentimes it feels like one good trip to Best Buy, and we could help solve this problem and be a whole lot better than where we are today.

There are a lot of questions that remain about what happened last month, and the uncertainty is very disconcerting to a host of people. And it's unacceptable to this committee and to the Congress. The most recent public reports indicate that many more Americans were affected by the breach than originally disclosed. Federal workers and their families deserve answers, answers on both the scope of the breach and the types of personnel information compromised.

Because of these many outstanding questions, we still don't understand the extent to which the breach threatens our national security. However, according to the intelligence community, the risk

is significant. Only the imagination limits what a foreign adversary can do with detailed information about a Federal employee's education, career, health, family, friends, neighbors, and personal habits.

I'd ask unanimous consent to enter into the record a letter we received on June 16 from the Federal Law Enforcement Officers Association.

I want to read part of it: Here are the concerns about the Office of Personnel Management data breaches, our demands of the government, and a list of questions that remain unanswered.

They represent some 28,000 current and retired Federal law enforcement officers and special agents from over 65 different agencies.

This is what they wrote: OPM turned its back on Federal law enforcement officers when they failed to protect sensitive information from an inexcusable breach. And OPM's delay and aloof response is a pathetic and irresponsible miscarriage of its obligations to affected Americans. The very lives of Federal law enforcement officers are now in danger, and their safety and security of innocent people, including their families, are now in jeopardy because of OPM's abysmal failure and its continued ignorance in the severity of the breach. The information lost includes personal, financial, and location information of these officers and their families, leaving them vulnerable to attack and retaliation for criminals and terrorists currently or formally investigated by the United States of America.

Without objection, I will enter this into the record.

Chairman CHAFFETZ. OPM is currently attempting to overhaul its technical infrastructure but without a full understanding of the scope or the cost of the project. In fact, the agency kept the project from the inspector general for more than a year. The IG determined OPM's chief information officer, "initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and cost of the effort required to mitigate it to the new environment." Because of these concerns, the project is, quote, "possibly making OPM environment less secure and increasing cost to taxpayers."

The IG also raised questions about why OPM awarded a sole-source contract for this project without going through the process for full and complete competition.

In fact, I would like to enter into the record without objection, this is an article from the Washington Post. This is May 13, "Defense Firm that Employed Drunk, High Contractors in Afghanistan May Have Wasted $135 Million in Taxpayer Dollars."

Chairman CHAFFETZ. These are the recipients of a sole-source contract to try to help clean up this mess. They were formally known as Jorge Scientific Corporation. They're now known as Imperatis Corporation. They have a good list of very impressive military personnel who are involved and engaged. Maybe this is the right decision. But when it is a sole-source contract, it does beg a lot of questions. No doubt we need to move fast. But this organization has had a lot of problems in the past, and it begs a lot of questions.

In addition to data security problem, we have a data management problem. It is unclear why so much background information related to security clearances was readily available on the OPM system to be hacked. It is unclear to me why there is a need for SF–86 background information—the SF–86 is the Standard Form 86. It's what the employees or prospective employees fill out. Why was this background information on the network if the applicant isn't currently being investigated?

Part of the reason we're in this mess and we have such a big mess in our hands is a lot of information and background checks that we're not even engaging in was still on the system. If information isn't accessible on the network, it can't be hacked. So if a security clearance isn't under investigation wall off the data. It's a best practice that others use and probably should have been used in this situation as well.

We have to do a better job of anticipating our adversaries and protecting information from unnecessary exposure. One of the concerns is this legacy system that we're using is a COBOL. The language used is COBOL. I'd ask unanimous consent to enter into the record a Wall Street Journal article from April 22, 1963, "COBOL Can Help Users Cut Costs When Changing Models; Government Spurs Progress." 1963. I wasn't even born yet. And that's the system that we're operating on in this day and age when technology is changing moment by moment, minute by minute.

Without objection, I will enter that into the record.

Chairman CHAFFETZ. Yesterday, Ms. Archuleta stated that no one is personally responsible for the OPM data breach and instead blamed the hackers. Hackers certainly have a lot of culpability on their hands. There's no doubt that there are nefarious actors that are going to be attacking the United States on a moment-by-moment basis. We literally take millions of hits on a daily basis. That's not new news. But I disagree that nobody is to be held personally responsible. Personal accountability is paramount. People have roles and responsibilities. They are charged with the fiduciary responsibility of carrying out those.

As the head of the agency, Ms. Archuleta is, in fact, statutorily responsible for the security of the OPM network and managing any risks. And while she may have inherited a lot of problems, she was called on by the President and confirmed by the Senate to protect the information maintained by OPM. During her confirmation in 2013, she stated that IT modernization would be one of her main priorities, yet it took a security breach in March of 2014, 5 months after the confirmation, to begin the process of developing a plan to fix the problem. That was just the beginning of the start to think about how to fix the problem. And yet the shift in blame is just inexcusable.

I really hope we hear solid answers. It's not going to be good enough to say: Oh, well, we'll get you that information. It's under investigation. There was a security—no. We're going to answer questions. Federal workforce, the people affected, they need to hear that. We're different. We're unique in this world because we are self-critical, and we do have hearings like this.

I would also ask unanimous consent to enter two letters into the record. One was the flash audit that was done, it was June 17 of

this year, from Patrick McFarland, the inspector general. It's a flash audit, U.S. Office of Personnel Management Information Improvement Project.

Without objection, I will enter that into the record.

Chairman CHAFFETZ. I will also ask unanimous consent to enter into the record the June 22 response by the Director of the Office of Personnel Management, Ms. Archuleta.

And I ask unanimous consent that enter into the record as well.

Without objection, so ordered.

Chairman CHAFFETZ. We also have some contractors here, and we appreciate their participation. They have answers—or we have questions that need to be answered as well. We need their cooperation to figure this out. A lot of what was done by OPM was contracted out. And there are very legitimate questions in particular that Mr. Cummings and others have asked that—and that's why I'm pleased to have them invited and participating as well. So it will be a full and robust committee hearing. And we appreciate all the participation.

As I conclude, I would also say, without objection, the chair is authorized to declare a recess at any time. I should have said that—without objection, so ordered. I should have said that at the beginning.

Now, I'd like to recognize the distinguished ranking member, Mr. Cummings, for his opening statement.

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

And this is a very important hearing. We're here today because foreign cyber spies are targeting millions of our Federal workers. OPM has made it clear that every month, there are 10 million efforts to pierce our cyberspace. These folks are hacking into our data system to get information about our employees, private information about them, their families, their friends, and all of their acquaintances. And they may try to use that information in their espionage efforts against United States' personnel and technologies.

Mr. Chairman, I want to start by thanking you. Last week, we held a hearing on cyber attacks against OPM. And this week, we have an opportunity to hear from OPM's two contractors that also suffered major data breaches, USIS and KeyPoint. Some people in your shoes might have merely criticized the agency without looking at the whole picture, but you agreed to my request to bring in the contractors. And you deserve credit for that, and I thank you.

On Monday night, I received a letter from USIS' representatives finally providing answers to questions I asked more than 7 months ago, Mr. Giannetta. Seven months ago. Seven months ago. Their letter disclosed that the breach at USIS affected not only DHS employees but our immigration agencies, our intelligence community, and even our police officers here on Capitol Hill.

But it took them 7 months, the night before the hearing, to give me that information but not only to give me the information but Members of Congress that information. My immediate concern was for the employees at these agencies. And I hope that they were all alerted promptly. But there's no doubt in my mind that USIS officials never would have provided that information unless they were called here to testify today.

So I thank you again, Mr. Chairman.

I have some difficult questions for USIS. I want to know why this company paid millions of dollars in bonuses to its top executives after the Justice Department brought suit against the company for allegedly—allegedly—defrauding the American taxpayers of hundreds of millions of dollars. I can hardly wait for the answer. I want to know why USIS used these funds for bonuses instead of investing in adequate cybersecurity protections for highly sensitive information our Nation entrusted to it.

Mr. Giannetta, I want to know if you as the chief information officer of USIS received one of those bonuses, and I'd love to know how much it was and what the justification for it was. I understand that you just returned from Italy. Welcome back. So this is probably the last place you want to be. I also understand you are leaving the company in a matter of weeks. But I want to know why USIS has refused for more than a year to provide answers to our questions about the board of directors of its parent company, Altegrity.

Mr. Hess, I also have difficult questions for you, for KeyPoint. At last week's hearing, I said one of our most important questions was whether these cyber attackers were able to penetrate OPM's networks using information they obtained from one of its contractors. As I asked last week, did they get the keys to OPM's networks from its contractor?

Yesterday, Director Archuleta answered that question. Appearing before the Senate Appropriations Committee, she testified, "The adversary leveraged a compromised KeyPoint user credential to gain access to OPM's network." So the weak link in this case was KeyPoint.

Mr. Hess, I want to know how this happened. I appreciate that OPM continues to have confidence in your company, but I also want to know why KeyPoint apparently did not have adequate logging capabilities to monitor the extent of data that was stolen. Why didn't you invest in these safe guards?

Mr. Chairman, to your credit, one of the first hearings you called after becoming chairman was on the risk of third-party contractors to our Nation's cybersecurity. At that hearing, on April 20, multiple experts explained that Federal agencies are only as strong as their weakest link. If contractors have inadequate safeguards, they place our government systems and our government workers at risk.

I understand that we have several individuals here sitting on the bench behind our panel of witnesses who may be called to answer questions if necessary: Mr. Job, who is the CIO of KeyPoint; and Mr. Ozment from the Department of Homeland Security.

Thank you, Mr. Chairman, for allowing them to be here.

As we move forward, it is critical that we work together. We need to share information, recognize when outdated legacy systems need to be updated, and acknowledge positive steps when they do occur. Above all, we must recognize that our real enemies are outside of these walls. They are the foreign nation-states and other actors that are behind these devastating attacks.

And, with that, I yield back.

Chairman CHAFFETZ. Thank the gentleman.

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

We're also pleased to have Representative Barbara Comstock, who is able to join us this morning.

And I ask unanimous consent that our colleague from Virginia be allowed to fully participate in today's hearing.

No objection. So ordered.

We now recognize the panel of witnesses. I'm pleased to welcome the Honorable Katherine Archuleta, Director of the Office of Personnel Management. We also have the Honorable Patrick McFarland, inspector general, the Office of Personnel Management; Ms. Donna Seymour, Chief Information Officer of the Office of Personnel Management; Ms. Ann Barron-DiCamillo—help me there, DiCamillo, just the way it's spelled—Director for the U.S. Computer Emergency Readiness Team at the United States Department of Homeland Security.

Appreciate you being here.

Mr. Eric Hess is the chief executive officer of KeyPoint Government Solutions. And Mr. Rob Giannetta is the chief information officer at USIS.

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

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

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

In order to allow time for discussion, please limit your verbal testimony to 5 minutes. And, obviously, your entire written record or written statement will be made part of the record.

We will start first with the Director of the Office of Personnel Management, Ms. Archuleta, first. You're now recognized for 5 minutes.

WITNESS STATEMENTS

STATEMENT OF THE HONORABLE KATHERINE ARCHULETA

Ms. ARCHULETA. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify before you again today.

I understand and I share the concerns and the frustration of Federal employees and those affected by the intrusions into OPM's IT systems. Although OPM has taken significant steps to meet our responsibility to secure personnel data of those we serve, it is clear that OPM needs to dramatically accelerate those efforts.

As I testified last week, I am committed to a full and complete investigation of these incidents. And we continue to move urgently to take action to mitigate the longstanding vulnerabilities of the agency's systems.

In March of 2014, we released our strategic IT plan to modernize and secure OPM's aging legacy system. We began implementing the plan immediately. And in fiscal years 2014 and 2015, we directed nearly $70 million toward the implementation of new security controls to better protect our systems. OPM is also in the proc-

ess of developing a new network infrastructure environment to improve the security of OPM infrastructure and IT systems.

Once completed, OPM IT systems will be migrated into this new environment from its current legacy networks. Many of the improvements have been to address critical immediate needs, such as security vulnerabilities in our network. These upgrades include the installation of additional firewalls, restriction of remote access without two-factor authentication, continuous monitoring of all connections to ensure that only legitimate connections have access, and deploying antimalware software across the environment to protect and prevent the deployment or execution of cybercrime tools that could compromise our networks.

These improvements led us to the discovery of the malicious activity that had occurred. And we were immediately able to share the information so that other agencies could protect their networks.

I also want to discuss data encryption. OPM does currently utilize encryption when possible. I have been advised by security experts that encryption in this instance would not have prevented the theft of this data because the malicious actors were able to steal privileged user accounts and credentials and could decrypt the data. Our IT security team is actively building new systems with technology that will allow OPM not only to better identify intrusions but to encrypt even more of our data.

In addition to new policies that were already implemented to centralize IT security duties under the CIO and to improve oversight of new major systems development, the IT plan recognized that further progress was needed. And the OIG's 2014 report credited OPM for progress in bolstering our security policies and our procedures and for committing critical resources to the effort.

With regard to information security governance, the OIG noted that OPM had implemented significant positive changes and removed its designation as a material weakness. This was encouraging, as IT governance is a pillar of the strategic IT plan. Regarding the weaknesses found with authorization, the OIG has recommended that I consider shutting down 11 out of the 47 OPM IT systems because they did not have current and valid authorization.

Shutting down systems would mean that retirees could not get paid and that new security clearances could not be issued. Of the systems raised in the 2014 audit, eleven of those systems were expired. Of those, one, a contractor system, is presently expired. All other systems raised in the 2014 audit have either been extended or provided a limited authorization.

OPM is offering credit monitoring services and identity theft information with CSID for the approximately 4.2 million current and former Federal civilian employees. Our team is continuing to work with CSID to make the online signup experience quicker and to reduce call center wait times. They are expanding staffing and call center hours and increasing server capacity.

I have taken steps to ensure that greater IT restrictions are in place, even for privileged users. That includes removing remote access for privileged users and requiring two-factor authentication. We're looking into further protections, such as tools that mask and redact data that would not be necessary for a privileged user to see.

I want to share with this committee some new steps that I am taking. First, I will be hiring a new cybersecurity adviser that will report directly to me. This cybersecurity adviser will work with OPM CIO to manage ongoing response to the recent incidents, complete development of OPM's plan to mitigate future incidents, and assess whether long-term changes to OPM's IT architecture are needed to ensure that its assets are secure. This individual is expected to be serving by August 1.

Second, to ensure that the agency is leveraging private sector best practices and expertise, I am reaching out to chief information security officers at leading private sector companies that experienced their own significant cybersecurity challenges. And I will host a meeting with these experts in the coming weeks to help identify further steps the agency can take. As you know, public and private sectors both face these challenges, and we should face them together.

I would like to address now the confusion regarding the number of people affected by two recent related cyber incidents at OPM. First, it is my responsibility to provide as accurate information as I can to Congress, the public, and, more importantly, the affected individuals. Second, because this information and its potential misuse concerns their lives, it is essential to identify the affected individuals as quickly as possible. Third, we face challenges in analyzing the data due to the form of the records and the way they are stored. As such, I have deployed a dedicated team to undertake this time-consuming analysis and instructed them to work—make sure their work is accurate and completed as quickly as possible.

As much as I want to have all the answers today, I do not want to be in a position of providing you or the affected individuals with potentially inaccurate data. With these considerations in mind, I want to clarify some of the reports that have appeared in the press. Some press accounts have suggested that the number of affected individuals has expanded from 4 million individuals to 18 million individuals. Other press accounts have asserted that 4 million individuals have been affected in the personnel file incident, and 18 million individuals have been affected in the background investigation incident. Therefore, I am providing the status as we know it today and reaffirming my commitment to providing more information as soon as we know it.

First, the two kinds of data that I'm addressing, personnel records and background investigations, were affected in two different systems in the two recent incidents. Second, the number of individuals with data compromised from the personnel records incident is approximately 4.2 million as reported on June 4. This number has not changed. And we have notified those individuals. Third, as I have noted, we continue to analyze the background investigation data as rapidly as possible to best understand what was compromised. And we are not at a point where we are able to provide a more definitive report on this issue.

That said, I want to address the figure of 18 million individuals that has been cited in the press. It is my understanding that the 18 million refers to a preliminary, unverified, and approximate number of unique Social Security numbers in the background investigations data. It is a number that I am not comfortable with

at this time because it does not represent the total number of affected individuals.

The Social Security number portion of the analysis is still under active review, and we do not have a more definitive number. Also, there may be an overlap between the individuals affected in the background incident and the personnel file incident. Additionally, we are working deliberately to determine if individuals who have not had their Social Security numbers compromised but may have other information exposed should be considered individuals affected by this incident.

For these reasons, I cannot yet provide a more definitive response on the number of individuals affected on the background investigation's data intrusion, and it may well increase from these initial reports. My team is conducting this further analysis with all due speed and care. And, again, I look forward to providing an accurate and complete response as soon as possible.

Thank you, Mr. Chairman, for this opportunity to testify today, and I'm happy to be here along with my CIO 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: Part II"

June 24, 2015

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

Thank you for the opportunity to testify before you again today. I want to be clear that I understand and I share the concerns and frustration of Federal employees and those affected by the intrusions into the U.S. Office of Personnel Management's (OPM's) information technology (IT) systems. As the Director of OPM, I know that the responsibility to secure the personal data of those we serve is of paramount importance. Although OPM has taken significant steps to meet our responsibility to secure the personal data of those we serve, it is clear that OPM needs to dramatically accelerate these efforts, not only for those individuals personally, but also as a matter of national security. As I testified last week, I am committed to a full and complete investigation of these incidents and we continue to move urgently to take action to mitigate the long-standing vulnerabilities of the agency's systems. I am also committed to providing the most up-to-date information to ensure affected individuals have the necessary resources and information available to protect their interests and security.

Strengthening OPM's IT Security

In March 2014, we released our *Strategic Information Technology Plan* to modernize and secure OPM's aging legacy system. The focus of the Plan is a set

Statement of The Honorable Katherine Archuleta
U.S. Office of Personnel Management

June 24, 2015

of strategic initiatives that will allow OPM to administer IT with greater efficiency, effectiveness, and security. This work recognizes recommendations from the U.S. Government Accountability Office and OPM's Office of Inspector General (OIG). Work to implement the Plan began immediately, and in Fiscal Years (FY) 2014 and 2015 we re-prioritized critical resources to direct nearly $70 million toward the implementation of tough new security controls to better protect our systems. OPM is also in the process of developing a new network infrastructure environment to improve the security of OPM infrastructure and IT systems. Once completed, OPM IT systems will be migrated into this new environment from the current legacy networks.

Many of the improvements have been to address critical immediate needs, such as the security vulnerabilities in our network. These upgrades include the installation of additional firewalls; restriction of remote access without two-factor authentication; continuous monitoring of all connections to ensure that only legitimate connections have access; and deploying anti-malware software across the environment to protect and prevent the deployment or execution of cyber-crime tools that could compromise our networks. These improvements led us to the discovery of the malicious activity that had occurred, and we were able to immediately share the information so that other agencies could protect their networks.

OPM thwarts millions of intrusion attempts on its networks in an average month. We are working around the clock to identify and mitigate security weaknesses. The reality is that integrating comprehensive security technologies into large, complex outdated IT systems is a lengthy and resource-intensive effort. It is a challenging reality, but one that we are determined to address. We have implemented these tools to the maximum extent possible, but the fact is that we were not able to deploy them before these two sophisticated incidents, and, even if we had been, no single system is immune to these types of attacks.

As we address critical immediate needs we also need to continue our work to improve long-term strategic challenges that affect our ability to ensure the security of our networks. I view the relationship that OPM has with our Inspector General as collaborative. We appreciate their recommendations and take them very seriously. As our OIG has noted, OPM has been challenged for several years in building and maintaining a strong management structure and the processes needed for a successful information technology security program. OPM agrees with this

assessment and it is this weakness that the Strategic IT Plan was developed to resolve.

I also want to discuss the important issue of data encryption. Though data encryption is a valuable protection method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection. OPM does currently utilize encryption when possible; however, due to the age of some of our legacy systems, data encryption is not always possible. In fact, I have been advised by security experts that encryption in this instance would not have prevented the theft of this data, because the malicious actors were able to steal privileged user credentials and could decrypt the data. Our IT security team is actively building new systems with technology that will allow OPM not only to better identify intrusions, but to encrypt even more of our data. Currently, we are increasing the types of methods utilized to encrypt our data.

In addition to new policies that were already being implemented to centralize IT security duties under the Chief Information Officer (CIO) and to improve oversight of new major systems development, the Plan recognized that further progress was needed. Thanks to OPM CIO Donna Seymour's leadership, the OIG's November 2014 audit credited OPM for progress in bolstering information technology security policies and procedures, and for committing critical resources to the effort.

Where the audit found weaknesses in Information Security Governance and Security Assessment and Authorization, OPM was already planning and implementing upgrades that emphasized improved security and the adoption of state of the art security protocols. Once these upgrades reached a mature stage in the spring of 2015, we were able to detect earlier intrusions into our data. Cybersecurity is fundamentally about risk management, and we must ensure that any recommendation helps us achieve the most effective level of cybersecurity and at the same time, allows us to continue providing critical services to the Federal workforce.

With regard to Information Security Governance, the OIG noted that OPM had implemented significant positive changes and removed its designation as a material weakness. This was encouraging, as IT governance is a pillar of the Strategic IT Plan. An enhanced IT governance capacity will identify and ensure we fund IT investments that are more tightly aligned with our needs. It will also allow us to manage, evaluate, measure, and monitor IT services in a more consistent and repeatable manner.

Regarding the weaknesses found with Security Assessment and Authorization, the OIG had recommended that I consider shutting down 11 out of 47 of OPM's IT systems because they did not have a current and valid Authorization. I am the leader of an organization that provides critical services to over two million current Federal employees around the world. The legacy systems that we are aggressively updating are critical to the provision of those services. Shutting down systems would mean that retirees would not get paid, and that new security clearances could not be issued. I am dedicated to ensuring that OPM does everything in its power to protect the federal workforce. But part of that included ensuring that our retirees receive the benefits they have earned and federal employees get the healthcare they need.

Of the systems raised in the FY 2014 audit report, eleven of those systems were expired. Of those, one, a contractor system, is presently expired. All other systems raised in the FY 2014 audit report have been either extended or provided a limited Authorization.

Addressing Federal Employees' Needs

For those approximately 4 million current and former Federal civilian employees who were potentially affected by the incident announced on June 4 regarding personnel information, OPM is offering credit monitoring services and identity theft insurance with CSID, a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services and is available immediately at no cost to affected individuals identified by OPM.

The high volume of notifications sent on the 18th and 19th of June, along with the a significant number of calls being made to the CSID call center from individuals who have not been impacted or notified of impact, caused wait times to increase, and those selecting on-line sign up at the end of last week experienced the CSID site timing out.

Our team is continuing to work with CSID to make the online signup experience quicker and to reduce call center wait times. These actions involve expanded staffing and call center hours, and increasing server capacity to better handle on-line sign ups at peak times. We continue to update our FAQ's on opm.gov to

address questions that we are getting from individuals who have or feel they may have been impacted.

Conclusion

The OIG's assessments of OPM's plans reflected the difficulties involved in working with complex legacy systems. This type of assessment is helpful to ensure OPM has the best, most comprehensive plans possible, and the OIG report helps everyone, including Congress, understand that these are complex issues that will require significant resources, both time and funding, to correct.

I would like to emphasize again that OPM has taken steps to ensure that greater restrictions are in place, even for privileged users. This includes removing remote access for privileged users and requiring two-factor authentication. We are looking into further protections, such as tools that mask and redact data that would not be necessary for a privileged user to see.

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

Chairman CHAFFETZ. Thank you.

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

STATEMENT OF THE HONORABLE PATRICK E. MCFARLAND

Mr. MCFARLAND. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, good morning. My name is Patrick McFarland, and I am the inspector general of the U.S. Office of Personnel Management. Thank you for inviting me to testify at today's hearing.

I would like to note that my colleague, Lewis Parker, the deputy assistant inspector general, is here with me. With your permission, he may assist in answering technical questions.

In 2014, OPM began a massive project to overhaul the agency's IT environment by building an entirely new infrastructure called the shell and migrating all of its systems to the shell from the existing infrastructure.

Before I discuss the OIG's recent examination of this project, I would like to make one point. There have been multiple statements made to the effect that this complete overhaul is necessary to address immediate security concerns because OPM's current legacy technology cannot be properly secured. This is not the case. There are many steps that can be taken or, indeed, which OPM has already taken to secure the agency's current IT environment. I just wanted to emphasize that while we agree that this overhaul is necessary, the urgency is not so great that the project cannot be managed in a controlled manner.

Last week, my office issued a flash audit alert discussing two significant issues related to this project. Because my written testimony describes these issues in detail, I will give only a summary for you this morning.

First, we have serious concerns with how the project is being implemented. OPM is not following proper IT project management procedures and does not know the true scope and cost of this project. The agency has not prepared a project charter, conducted a feasibility study, or identified all of the applications that will have to be moved from the existing IT infrastructure to the new shell environment.

Further, the agency has not prepared the mandatory OMB Major IT Business Case, formally known as Exhibit 300. This document is an important step in the planning of any large-scale IT project as it is the proper vehicle for seeking approval and funding from OMB. It is also a necessary process for enforcing proper project management techniques.

Because OPM has not conducted these very basic planning steps, it does not know the true cost of the project and cannot provide an accurate timeframe for completion. OPM has estimated that this project will cost $93 million. However, the amount only includes strengthening the agency's current IT security posture and the creation of a new shell environment. It does not include the cost of migrating all of OPM's almost 50 major IT systems and numerous subsystems to the shell.

This migration will be the most costly and complex phase of this project. Even if the $93 million figure was an accurate estimate, the agency does not have a dedicated funding stream for the

project. Therefore, it is entirely possible that OPM could run out of funds before completion, leaving the agency's IT environment more vulnerable than it is now.

OPM also has set what I believe to be an unrealistic timeframe for completion. The agency believes it will take approximately 18 to 24 months to migrate all of its systems to the shell. It is difficult to imagine how OPM will meet the goal when it does not have a comprehensive list of all the systems that need to be migrated. Further, this process is inherently difficult, and there are likely to be significant challenges ahead.

The second major point discussed in the alert relates to the use of sole-source contract. OPM is contracted with a single vendor to complete all four phases of this project. Unless there is a specific exception, Federal contracts must be subject to full and open competition. However, there's an exception for compelling and urgent situations.

The first phase of this project, which involves securing OPM's IT environment, was indeed such a compelling and urgent situation. That phase addressed a crisis, namely the breaches that occurred last year. However, the later phases, such as migrating the application to the new shell environment, are not as urgent. Instead, they involve work that is essentially a long-term capital investment.

It may sound counterintuitive, but OPM should step back, complete its assessment of its current IT architecture and develop an OMB major IT business case proposal. When OMB approval and funding have been secured, OPM should move forward with the project in a controlled manner using sound project management techniques. OPM cannot afford to have this project fail.

I fully support OPM's effort to modernize its IT environment and the Director's long-term goals. However, if it is not done correctly, the agency will be in a worse situation than it is today and millions of taxpayer dollars will have been wasted.

I'm happy to answer any questions you may have.

[Prepared statement of Mr. McFarland follows:]

Office of the Inspector General
United States Office of Personnel Management

Statement of the Honorable
Patrick E. McFarland
Inspector General

before the

Committee on Oversight and Government Reform

United States House of Representatives

on

"OPM Data Breach: Part II"

June 24, 2015

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

Good morning. My name is Patrick E. McFarland. I am the Inspector General of the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing.

Before I begin, I would like to clarify two points that were discussed before this Committee on Tuesday, June 16, 2015. First, there were several statements made that OPM's legacy information systems are supported by very old technology (specifically COBOL, a mainframe programming language), and therefore could not be protected by modern security controls. However, we know from our audit work that some of the OPM systems involved in the data breaches run on modern operating and database management systems. Consequently, modern security technology such as encryption or data loss prevention could have been implemented on these specific systems.

Also, OPM has stated that because the agency's IT environment is based on legacy technology, it is necessary to complete a full overhaul of the existing technical infrastructure in order to address the immediate security concerns. While we agree in principle that this is an ideal future goal for the agency's IT environment, there are steps that OPM can take (or has already taken) to secure its current IT environment.

For example, OPM has significantly upgraded security controls to protect the perimeter of its network and prevent the type of attacks that occurred in 2014. In addition, some of OPM's most sensitive systems are compatible with additional security controls such as data encryption and other data loss prevention techniques could be utilized to protect OPM's systems. Moreover, implementing full two-factor authentication to access OPM's major IT systems will add an additional layer of defense that will go a long way toward preventing additional data breaches.

Second, at the hearing last week it was also stated that all information systems that we identified as not having a current Authorization in the FY 2014 FISMA report have since been Authorized. I believe that the comments were in reference to a memorandum issued by the Chief Information Officer (CIO) in April 2015 that granted an extension of the previous Authorization for the 11 systems in question. However, in its annual Federal Information Security Management Act (FISMA) reporting guidance, the Office of Management and Budget (OMB) specifically states that an "extended" or "interim" Authorization is not valid; therefore, these systems are not in fact Authorized.[1]

In addition, the CIO's memorandum does not resolve the primary concern. The Authorization itself is a formal document that grants permission for an information system to operate in a production environment. The *process* of Authorization is the relevant issue, since it involves a comprehensive assessment of a system's security level, risks, and controls. The fact remains that this process has not been completed for the 11 systems identified in the Fiscal Year (FY) 2014 FISMA audit report.[2]

OPM's Infrastructure Overhaul Project

In April 2014, in response to the March 2014 breach, OPM initiated a major IT overhaul. The initial plan was to make major security improvements to the existing environment and continue to operate OPM systems in their current location. During the process of implementing security upgrades, OPM determined that it would be more effective to completely overhaul the agency's

[1] 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.

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

IT infrastructure and architecture and move it into an entirely new environment (referred to as the Shell).

There are four phases in the Project:

- Tactical – shoring up the existing security environment
- Shell – creating the new data centers and IT architecture
- Migration – migrating all OPM systems to the new environment
- Clean-up – decommissioning existing hardware and systems

Our understanding is that the Tactical phase was completed in April 2015 and the Shell phase is underway and is expected to be completed this fall.

We support OPM's efforts to modernize and better secure its IT environment; however, we have two significant concerns with this Project, resulting in an issuance of a Flash Audit Alert.

Flash Audit Alert

The typical audit process can take up to 10 to 12 months from the start of the audit to the issuance of the final report. As part of our normal audit process, we provide a draft audit report to OPM for comment. It is a fact finding step to ensure that our audit field work is complete and accurate. We consider those comments, make any necessary changes, and incorporate them into our final audit report.

However, sometimes in the course of our work, we discover significant evidence of a critical problem that needs *immediate* attention by OPM. In those situations, we issue what is called a "Flash Audit Alert." We do not normally provide a draft of this alert to the agency for comment given the time sensitive nature of the matter.

After our auditors finished conducting their initial review of the Project, we determined (1) the situation was serious enough to issue a Flash Audit Alert and (2) because of the significance of the Project, we would provide the agency with a brief window to provide comments on the draft alert.

We provided a draft copy of our Flash Audit Alert to the Office of the Chief Information Officer (OCIO) on June 2, 2015, after verbally briefing the CIO several days before. We requested comments by June 5th, and later extended that to June 10th. By June 17th we still had not received comments, or indication that comments would be forthcoming. Because of the urgency of the situation, I issued the Flash Audit Alert without the benefit of agency comments.

The two primary concerns discussed in the Flash Audit Alert relate to (1) project management and (2) the use of a sole-source contract.

1. Project Management Activities

The most significant shortcoming of OPM's management of the Project is that it has not prepared a "Major IT Business Case" proposal (formerly known as the OMB Exhibit 300), as required by OMB for IT projects of this size and scope. Preparing an OMB proposal would require OPM to fully evaluate the costs, benefits, and risks associated with its planned Project, and present its business case to OMB to seek approval and funding.

OMB Circular A-11 Appendix 6 defines capital budgeting requirements for capital asset projects. The basic concepts are that capital asset projects require proper planning, cost/benefit analysis, financing, and risk management. This includes demonstrating that the return on investment exceeds the cost of funds used, and that the full cost of the project is appropriated before work begins. Finally, the Circular requires risk management and earned value management throughout the life-cycle of the Project to ensure that it continues to meet cost and schedule targets.

For OPM to complete this process it must first fully determine the true scope and cost of the project. However, we learned from our audit work that OPM is still evaluating its existing IT architecture, including the identification of all mainframe applications that will need to be migrated to the Shell environment. Further, other systems will need to be redesigned before they can be migrated. There are approximately 50 major IT systems in OPM's inventory, and a large number of related sub-systems. Until this evaluation is complete, OPM is not able to estimate how long it will take or how much it will cost to complete the Migration phase of the Project.

Despite this, OPM officials informed us that the Migration phase will be complete in 18 to 24 months. We believe that OPM is highly unlikely to meet this target. Many critical OPM applications (including those that process annuity payments for Federal retirees, reimburse health insurance companies for claims payments, and manage background investigations) run on OPM's mainframe computers. These applications are based on legacy technology, and will need to be completely renovated to be compatible with OPM's proposed new IT architecture.

This will be a highly complex and monumental task. OPM has a history of troubled system development projects. Despite multiple attempts OPM has failed to modernize its retirement claims processing system. Although the 2009 revamp of OPM's financial system (now called CBIS) was ultimately partially successful, it was also fraught with difficulty. The CBIS project was the main focus of agency leadership at that time. It was relatively well managed, and was subject to oversight from several independent entities, including my office, but it still required two years and over $30 million to complete.

OPM's current initiative will be far more complex than anything OPM has attempted in the past, since each individual application migration should be treated as its own project similar to these examples. Furthermore, there are many other systems besides OPM's mainframe applications that will also need to be modified to some extent to be compatible with the Shell environment.

Even more troubling is the fact that OPM has not followed basic best practices for program management including developing a project charter, a comprehensive list of stakeholders, a feasibility study and impact assessment, test plans, and other standard project management artifacts.

In addition to defining cost and schedule targets, the OMB Major IT Business Case process is intended to secure funding for major IT investments before work begins. However, OPM has already committed substantial funds toward this project without completing the process. In FY 2015 OPM has obligated approximately $32 million toward shoring up its existing IT security controls and establishing the Shell environment. In its FY 2016 budget request, OPM requested and received an additional $21 million from OMB for the Project.

OPM program officials told us that some of the Project's funding will come from the $21 million budget request, $5 million from the U.S. Department of Homeland Security, and from assessments on the program offices. In addition, program offices will be required to fund the migration of applications they own from their existing budgets. However, program office budgets are intended to fund OPM's core operations, not subsidize a major IT infrastructure project.

It is unlikely that OPM will be able to fund the substantial migration costs related to this Project without a significantly adverse impact on its mission unless it seeks dedicated funding through Congressional appropriation. Also, OPM's current budget approach seems to violate IT spending transparency principles promoted by OMB's budget guidance and its IT Dashboard initiative, which is intended to "shine [a] light onto the performance and spending of IT investments across the Federal Government."

Without a dedicated funding stream, there is a very high risk that funding will be inadequate to support the entire Migration phase, which is likely to be complex, time consuming, and extremely expensive. In addition, without the disciplined project management processes that are associated with the OMB Major IT Business Case process, there is a high risk that this Project will fail to meet all of its stated objectives. In this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers. This outcome would be contrary to the stated goals of creating a more secure IT environment at a lower cost.

The best chance for a successful modernization of OPM's IT environment is to develop and execute a comprehensive plan based on accepted project management disciplined processes.

2. Sole-Source Contract

OPM has secured a sole-source contract with a vendor to manage the infrastructure improvement project from start to finish. Although OPM completed a Justification for Other Than Full and Open Competition (JOFOC) to justify this contract, we do not agree that it is appropriate to use this contract for the entire Project.

The initial phase of the Project covered the procurement, installation, and configuration of a variety of software tools designed to improve the IT security posture of the agency (the Tactical phase). We agree that recent security breaches at OPM warranted a thorough and immediate reaction to secure the existing environment, and that the JOFOC was appropriate for this activity. However, we do not agree that it is appropriate to use a sole-source contract for the long-term system development and migration efforts.

OPM officials informed us that the reason for using the sole-source contract for the long term was to ensure continuity. The OCIO believes the same vendor that helped build the infrastructure should be responsible for migrating applications into that environment.

Federal Acquisition Regulation § 6.302 outlines seven scenarios where contracting without full and open competition may be appropriate, two of which relate to an unusual and compelling urgency and national security implications. There is no exception to the requirement for full and open competition for vendor continuity for the convenience of the agency.

The current vendor may well be chosen as the successful bidder through full and open competition when the Migration and Clean-up phases begin. Without subjecting the remainder of this process to competition, there is a high risk that project costs will be inflated. Further, it is highly unlikely that any single vendor is qualified for the Migration phase. OPM's information systems are supported by a wide variety of operating systems, databases, and programming languages. Each individual application migration will likely require dedicated contractor support by a vendor that specializes in the specific technology supporting that system.

The Migration and Clean-up phases are not responses to a crisis situation, as the Tactical phase was. Therefore, we believe that OPM should subject the remainder of the project to contracting vehicles other than the sole-source contract used for the Tactical and Shell phases.

Conclusion

While I fully support OPM's efforts to modernize its IT environment, I am concerned that there is a high risk that its efforts will ultimately be unsuccessful. For example, if the Migration phase fails, the results could be catastrophic. The agency could end up with half of its systems in the new Shell environment and half of its systems in the legacy environment. Neither of the environments would be fully secure, and OPM would be in a position where it is forced to pay indefinitely for the overhead costs of both infrastructures.

System development projects by their very nature are complex and prone to failure. Even with the application of strict project management techniques, many projects either fail entirely, or are only partially successful. Even so, there is a chance that this effort will ultimately succeed given time, leadership, and strong project management.

I am happy to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

Ms. Seymour, was your statement with Ms. Archuleta, or do you have one yourself?

Ms. SEYMOUR. It was with the Director. Thank you, sir.

Chairman CHAFFETZ. Okay. Very good.

I would ask unanimous consent to enter into the record a letter that was given us this morning from the Office of Personnel Management. It's dated today, signed by Ms. Archuleta, dealing with the number of records.

Without objection, so ordered. We'll enter that into the record.

Chairman CHAFFETZ. We'll now recognize Ms. Barron-DiCamillo for 5 minutes.

STATEMENT OF ANN BARRON–DICAMILLO

Ms. BARRON-DICAMILLO. Thank you. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, good morning. My name is Ann Barron-DiCamillo. I appear here today to talk about the role that my organization, the United States Computer Emergency and Readiness Team, known as US–CERT, played in the recent breaches involving OPM.

As stated by Ranking Member Cummings, Assistant Secretary Dr. Andy Ozment, is also here with me to answer any questions.

Like many Americans, I, too, am victim of these incidents and concerned about the continued cyber incidents at numerous government and private sector entities. I am a career civil servant who has worked to improve the security of critical government and private sector networks for the past 13 years. I understand both the scope and the problem we face and the challenges in securing critical networks.

Cybersecurity is a true team sport. There are many different agencies responsible for aspects of cybersecurity, including members of the intelligence community, law enforcement, the Department of Homeland Security, as well as individual system owners, and individual end users as well. My organization within DHS, the US–CERT, is part of the National CyberSecurity and Communications Integration Center, also known as an NCCIC.

US–CERT focuses on analyzing the evolving cyber risks, sharing information about threats and vulnerabilities, and responding to significant cyber incidents. We work with trusted partners around the world and focus on threats and incidents facing the government and critical private sector networks. In both cases, our role is largely voluntary. We build and rely upon trusted relationships to both share information and respond to incidents.

When an entity believes that they have been a victim of a significant cyber incident, they often invite us to help them assess the scope of any intrusion as well as provide recommendations on how they can mitigate the incident and improve their security posture going forward. US–CERT's current involvement with OPM began in March of 2014, when we first learned that there was a potential compromise within the OPM networks.

From March through May of 2014, US–CERT was part of an interagency response team that first assessed the scope of the malicious activity and then remediated that intrusion. Throughout that time, US–CERT shared information that we had learned about the

intrusion with our governmental partners as well as private sector partners, so that they too could better protect themselves.

We also created signatures so that our EINSTEIN systems could look for malicious activity at other Federal agencies. On May 28, 2014, the interagency response team concluded that the malicious actor in question from that event had been removed from the network. US–CERT also provided OPM with recommendations about what steps they could take to increase their own security.

It is important to note that there is no silver bullet or magic solution to secure networks from a sophisticated actor. Most government agencies and their private sector counterparts are making up for years of underspending on security as part of the information technology development. As many experts have noted, the Internet was designed with ease of use rather than security in mind.

The status of OPM networks in May of 2014 was not unlike other similarly situated agencies. OPM did some things well and was weak in other areas. I understand that OPM had at the time under its new leadership just started an effort to improve its cybersecurity. The US–CERT incident report for OPM included several specific mitigation recommendations, some of which could be implemented fairly quickly and others of which would take longer.

From what I observed, OPM made a concerted effort to adopt the US–CERT recommendations beginning last summer. Indeed, it was OPM who, in April of 2015, discovered the current intrusion on its own networks using one of the tools recommended by US–CERT. Based on the OPM discovery, US–CERT created new EINSTEIN signatures to look for similar intrusions at other agencies. This is how the malicious access to OPM data at the Department of Interior data center was discovered. This newly discovered threat information was also quickly shared by US–CERT with out private sector partners and other trusted partners around our communities.

US–CERT and the interagency response team have been working with OPM since April of 2015 to assess the nature and scope of the incident. While the investigation is ongoing, there are a few things that I can share. We were able to use the EINSTEIN capabilities to detect the presence of malicious activity on the Department of the Interior data center, which houses the OPM personal records.

Further onsite investigation revealed that some OPM personal data was compromised and see that at least some of that data had been exfiltrated by the Department of the Interior data center. This is the 4.2 million number that Director Archuleta has referenced today. As a result of what we learned from the April 2015 investigation, OPM continued to conduct forensic investigations into its own environment.

In that process, OPM discovered evidence of an additional compromise on its own network. US–CERT then led another interagency response team to assess OPM's networks and, in early June, found that background investigation data had been exposed and possibly exfiltrated. Again, that's currently under investigation.

We also learned at the time that OPM's ongoing efforts to implement two-factor authentication had precluded continued access by the intruder into the OPM network. This protected measure, like others instituted by OPM, may have mitigated any continued ef-

fects of the intrusion. The work of the interagency response team is ongoing, and we continue to assess the scope of the potential compromise.

Although I am appearing today ready to provide information to this committee, I do so with some concern. As I had mentioned, US–CERT relies on voluntary cooperation from agencies and private entities who believe that they may be victims of malicious activity. I worry that US–CERT appearing before this committee will have a chilling effect on their willingness to notify us, the whole of government, of future incidents. We especially need private companies to continue to work with government and to share information about cyber threats and incidents so that, through greater shared awareness, we can all be more secure from those who seek to do us harm.

Thank you, and I look forward to your questions.

Chairman CHAFFETZ. Thank you.

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

STATEMENT OF ERIC A. HESS

Mr. HESS. Thank you, Chairman Chaffetz, Ranking Member Cummings, and members of the committee. My name is Eric Hess. I am president and chief executive officer of KeyPoint Government Solutions.

Since 2004, KeyPoint has provided fieldwork services for the background investigations to a number of Federal agencies, including the Office of Personnel Management. KeyPoint, which employs investigators in every State, is proud to be part of OPM's team helping to ensure that security clearance investigations it conducts are thorough, detailed, and consistent.

KeyPoint takes issues of cybersecurity very seriously. And as a contractor providing critical services across the Federal Government, we stand in partnership with the Federal Government in trying to combat ever-present and ever-changing cyber threats. KeyPoint is committed to ensuring the highest levels of protection for sensitive information in which we are entrusted.

The recently announced breach at OPM is the focus of this hearing. With that in mind, I would like to make clear that we see no evidence suggesting KeyPoint was in any way responsible for the OPM breach. There have been some recent media reports suggesting that the incursion into OPM's systems last year is what facilitated the recent announced OPM breach. There is absolutely no evidence that KeyPoint was responsible for that breach.

The press have also reported the hackers stole OPM credentials assigned to a KeyPoint employee and leveraging to access OPM systems. As Director Archuleta noted at the Senate hearing yesterday, there was no evidence suggesting that KeyPoint is responsible for or directly involved with the incursion. To be clear, the employee was working on an OPM system, not a KeyPoint system.

Now, I know that, during this hearing, the incursion of KeyPoint system that was discovered last September will also be discussed. Before going into more detail, I would like to note that KeyPoint has continuously maintained its authority to operate ATO from OPM and DHS. This means that we met the stringent information and security requirements imposed under our Federal contracts.

KeyPoint only maintains personal information that is required under our contractual obligations. However, we, like government agencies, face aggressive, well-funded, and ever-evolving threats that require us to exceed the current FISMA requirements in order to protect the sensitive information in our charge.

Let me say a few words about the earlier incursion of KeyPoint. In December of 2014, the Washington Post reported that OPM had announced it would notify over 48,000 Federal workers that their personal information may have been exposed as a result of incursion to KeyPoint systems. I emphasize the word "may" because in the report, after the extensive analysis of the incursion, we find no evidence of exfiltration of sensitive personal data.

Last August, following public reports of a data security breach at another Federal contractor providing background checks, OPM Chief Information Officer Donna Seymour asked KeyPoint to invite the United States Computer Emergency Readiness Team, or US–CERT, to test KeyPoint's network and KeyPoint agreed. The team from the Department of Homeland Security National Cybersecurity Assessment and Technical Services conducted risk vulnerability assessment. The NCATS team conducted full network and application vulnerability tests of KeyPoint systems, including network mapping, internal and external penetration testing.

The NCATS team provided a number of findings at the end of the engagement, which were resolved while the team was on site, as well as recommendations for the future. Ultimately, while the NCATS team found issues, they were resolved, and the team found no malware or KeyPoint system.

However, then in September, the US–CERT Hunt team informed KeyPoint that it had found indications of the sophisticated malware undetectable by commercial antivirus on two computers. The US–CERT team provided KeyPoint with mitigation recommendations to remove the malware from our environment and other recommendations for hardening its network to prevent and defeat future compromises.

KeyPoint acted quickly and immediately began implementing the recommendations. KeyPoint conducted an internal investigation of the data security issues identified by US–CERT and concluded that the malware in question was not functioning correctly, potentially caused by errors made during its installation on KeyPoint system. Again, neither US–CERT's investigation nor ours found any evidence of exfiltration of personally identifiable information.

I recently attended a classified briefing at OPM where I learned more about the OPM breach. In this open setting, I cannot go into details that were presented in that briefing. However, I can reiterate that we have seen no evidence of connection between the incursion at KeyPoint and the OPM breach that's the subject of this hearing. That said, we are always striving to ensure KeyPoint cyber defenses are as strong as possible, and we welcome US–CERT's recommendation for strengthening the security of our system.

We've also been working closely with OPM and CBP to improve our information security posture in light of the new advanced persistent threats. OPM presented us with a 90-day network hardening plan. We completed it. We have been working diligently to

make our systems more resilient and stronger by implementing the US–CERT recommendations. And a number of the most significant improvements we put into place are full deployment of multifactor authentication; Security Information Events Management; enhanced intrusion detection systems; NetFlow and packet capture network information; improved network segmentation; and many more.

Additionally, we've been working with all of our customers to update our ATOs. This process includes an audit from a third-party independent 3PAO assessor.

In closing, cybersecurity is vital to KeyPoint's mission, and we will continue to fortify protections of our systems. Our adversaries are constantly working to create new methods of attack against our systems, and we must constantly work to meet and deter those attacks. While it may be impossible to ever truly eliminate the threat of cyber attack, we will continue to evaluate our protections and ensure that they reflect the most current best practices.

I want to thank the committee for drawing attention to this critical issue and for allowing KeyPoint to share its perspective with the committee today. I look forward to your questions.

[Prepared statement of Mr. Hess follows:]

Eric Hess, CEO, KeyPoint Government Solutions
"OPM Data Breach: Part II"
House Committee on Oversight and Government Reform
June 24, 2015

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, my name is Eric Hess, and I am President and Chief Executive Officer of KeyPoint Government Solutions ("KeyPoint").

Since 2004, KeyPoint has provided fieldwork services for background investigations to a number of federal agencies, including the Office of Personnel Management ("OPM"). KeyPoint, which employs investigators in every state, is proud to be part of OPM's team, helping to ensure that the security clearance investigations it conducts are thorough, detailed, and consistent. KeyPoint takes issues of cybersecurity very seriously and, as a contractor providing critical services across the federal government, we stand in partnership with the federal government in trying to combat ever-present and ever-changing cyber-threats. KeyPoint is committed to ensuring the highest levels of protection for the sensitive information with which we are entrusted.

The recently-announced data breach at OPM is the focus of this hearing. With that in mind, I would like to make clear that we have seen no evidence suggesting KeyPoint was in any way responsible for the OPM breach. There have been some recent media reports suggesting that the incursion into KeyPoint's system last year is what facilitated the recently-announced OPM breach. There is absolutely no evidence that KeyPoint was responsible for that breach. The press also has reported that hackers stole OPM credentials assigned to a KeyPoint employee and leveraged them to access OPM's systems. As Director Archuleta noted at a Senate hearing yesterday, there is no evidence suggesting that KeyPoint was responsible for or directly involved in the incursion. To be clear, the employee was working on OPM's systems, not KeyPoint's.

Now, I know that during this hearing, the incursion into the KeyPoint system that was discovered last September will also be discussed. Before going into more detail, I would note that KeyPoint has continuously maintained its Authority to Operate (known as an ATO) from OPM and from DHS (under our TSA contract and more recently our CBP contract). This means we met the stringent information security requirements imposed under our federal contracts. KeyPoint only maintains personal information that is required under our contractual obligations. However, we, like the government, face aggressive, well-funded and ever-evolving threats that require us to exceed current FISMA requirements in order to protect the sensitive information in our charge.

So let me say a few words about the earlier incursion of the KeyPoint system. In December 2014, *The Washington Post* reported that OPM had announced it would notify over 48,000 federal workers that their personal information "*may* have been exposed" as the result of an incursion into KeyPoint's systems.[1] I emphasize the word "may" in the report because, after an

[1] Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, THE WASHINGTON POST, Dec. 18, 2014, http://www.washingtonpost.com/business/economy/keypoint-suffers-

(Cont'd on next page)

extensive analysis of this incursion, we found no evidence of the exfiltration of sensitive personal data.

Last August, following public reports of a data security breach at another federal contractor providing background checks, OPM Chief Information Officer Donna Seymour asked KeyPoint to invite the United States Computer Emergency Readiness Team, or US-CERT, to test KeyPoint's network, and KeyPoint agreed. A team from the Department of Homeland Security National Cybersecurity Assessment and Technical Services ("NCATS") conducted a Risk and Vulnerability Assessment ("RVA"). The NCATS team conducted a full network and application vulnerability test of KeyPoint's systems, including network mapping and internal and external penetration testing. The NCATS team provided a number of findings at the end of its engagement, which were resolved while the team was onsite, as well as recommendations for the future. Ultimately, while the NCATS team found issues, they have been resolved and the team found no malware on KeyPoint's network.

Then in September, the US-CERT Hunt team informed KeyPoint that it had found indications of sophisticated malware undetectable by commercial antivirus on two computers. The US-CERT team provided KeyPoint with a mitigation recommendation to remove the malware from the environment and other recommendations on hardening its network to prevent and detect future compromises. KeyPoint acted quickly and immediately began implementing the recommendations.

KeyPoint conducted an internal investigation of the data security issues identified by US-CERT and concluded that the malware in question was not functioning correctly, potentially caused by errors made when it was installed on KeyPoint's systems. Again, neither US-CERT's investigation, nor our investigation found evidence of the exfiltration of sensitive personal information.

I recently attended a classified briefing at OPM, where I learned more about the OPM breach. In this open setting, I cannot go into the details that were presented in that briefing, however, I can reiterate that we have seen no evidence of a connection between the incursion at KeyPoint and the OPM breach that is the subject of this hearing.

That said, we are always striving to ensure that KeyPoint's cyber-defenses are as strong as possible, and we welcomed US-CERT's recommendations for strengthening the security of our system. We have also been working closely with our customers OPM and CBP to improve our information security posture in light of new advanced persistent threats. OPM presented us with a 90-day network hardening plan. We completed it. We have been working diligently to make our systems more resilient and stronger by implementing the US-CERT recommendations. A number of the most significant improvements we put into place are as follows:

(Cont'd from previous page)

network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html (emphasis added).

- **Full Deployment of Multifactor Authentication** to login to our laptops, KeyPoint VPN connections, and PIV authentication for all VPN access to the OPM network.
- **Security Information and Event Management (SIEM),** which centralizes logging and alerting of all network and system events.
- **Enhanced Intrusion Detection System (IDS)** – improving our IDS capability that monitors the network for malicious activities and produces alerts and reports to a management station.
- **NetFlow and Packet Capture (PCAP) Network Information** – collection and retention of data to provide detailed analysis of IP network traffic for any future forensic investigations.
- **Improved Network Segmentation** – upgrading our existing segmentation to include customer level isolation.
- **And many more…**

Additionally, we have been working with all our customers to update our ATOs. This process includes an audit from a third party independent 3PAO assessor.

In closing, cybersecurity is vital to KeyPoint's mission, and we will continue to fortify the protection of our systems and information. Our adversaries are constantly working to create new methods of attack against our systems, and we must constantly work to meet and deter those attacks. While it may be impossible to ever truly eliminate the threat of a cyber-attack, we will continue to evaluate our protections to ensure they reflect the most current "best practices."

I want to thank the committee for drawing attention to this critical issue, and for allowing KeyPoint to share its perspective with the committee today. I look forward to addressing your questions.

Chairman CHAFFETZ. Thank you for your testimony.

Mr. Giannetta, we will now recognize you for 5 minutes.

STATEMENT OF ROB GIANNETTA

Mr. GIANNETTA. Thank you. Good morning, Mr. Chairman, Ranking Member Cummings, and members of the committee. My name is Robert Giannetta, and I'm currently the chief information officer at US Investigations Services, LLC, which is often referred to as USIS or USIS. I joined USIS as the CIO in August 2013. Before then, I was with BAE Systems, Nextel, and Verizon. I also served in the United States Navy.

Until August 2014, USIS performed background investigation work for the United States Office of Personnel Management. When I started working at USIS, the information technology systems it used to perform OPM background investigation work were operating under two security certifications, known as authorities to operate, which issued from OPM in 2012. Those authorities to operate required annual review of USIS systems. OPM's 2014 review included approval of USIS system security plans and a site visit in May of 2014.

In June 2014, USIS self-detected a cyber attack on its information technology systems. USIS immediately notified OPM and initiated a comprehensive response plan pursuant to USIS' written OPM-approved incident response plan. USIS' response included retaining the highly regarded independent forensics investigations firm Stroz Friedberg to lead the investigation and remediation efforts.

USIS instructed Stroz Friedberg to leave no stone unturned in their investigation. USIS invested thousands of person hours and millions of dollars to investigate and remediate against the attack. By early June 2014, those efforts succeeded in blocking and containing the attacker.

The Stroz investigation was also able to develop significant technical details about how the attack occurred, what the attacker did within the USIS systems, and which systems and data were potentially compromised. All of this information was openly shared with OPM as well as other government agencies.

In addition, USIS invited US–CERT and other government investigators into its facilities in late July 2014 and gave them full access to USIS systems. In August 2014, OPM issued a stop-work order to USIS and subsequently terminated its longstanding contractual relationship with the company. This led USIS to exit the background investigation business and ultimately to bankruptcy.

Just yesterday, I was invited to appear to testify before the committee. I'll do my best to answer any questions you may have. Thank you.

[Prepared statement of Mr. Giannetta follows:]

ROBERT W. GIANNETTA, SR.
CHIEF INFORMATION OFFICER
US INVESTIGATIONS SERVICES, LLC

My name is Robert W. Giannetta, Sr.

I am the Chief Information Officer of US Investigations Services, LLC, which is often referred to as USIS. I joined USIS as the CIO in August 2013. Before then, I was with BAE Systems, Nextel, and Verizon. I also served in the United States Navy.

Until August 2014, USIS performed background investigations work for the United States Office of Personnel Management. When I started working at USIS, the information technology systems used to perform OPM background investigations work were operating under two security certifications (known as Authorities to Operate), which issued from OPM in 2012. Those Authorities to Operate required annual review of USIS systems. OPM's 2014 review included approval of USIS's Systems Security Plans and a site visit in May 2014.

In June 2014, USIS self-detected a cyber attack on its information technology systems. USIS immediately notified OPM and initiated a comprehensive response pursuant to USIS's written, OPM-approved Incident Response Plan.

USIS's response included retaining the highly regarded, independent forensics investigation firm Stroz Friedberg to lead the investigation and remediation efforts. USIS instructed Stroz Friedberg to leave no stone unturned in their investigation. USIS invested thousands of person-hours and millions of dollars to investigate and remediate against the cyber attack on USIS systems. By early July 2014, those efforts succeeded in blocking and containing the attacker.

The Stroz investigation also was able to develop significant technical details about how the attack occurred, what the attacker did within USIS's systems, and which systems and data were potentially compromised. All of this information was openly shared with OPM, as well as other government agencies. In addition, USIS invited US-CERT and other government investigators into its facilities in late July 2014 and gave them full access to USIS's systems.

In August 2014, OPM issued a stop work order to USIS and subsequently terminated its longstanding contractual relationships with USIS. This led USIS to exit the background investigations business and ultimately to bankruptcy.

Just yesterday, I was invited to appear to testify before the Committee. I will do my best to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

I now recognize myself. Ms. Archuleta, you have personal identifiable information for how many Federal employees and retirees?

Ms. ARCHULETA. We have——

Chairman CHAFFETZ. Move your microphone closer, please.

Ms. ARCHULETA. We have 2.7 individuals who were full-time employees and 2.4 who are——

Chairman CHAFFETZ. No, I asked you how many—you have personally identifiable information for how many Federal employees and retirees?

Ms. ARCHULETA. The number I just gave you includes the number of employees and retirees. And personally identifiable information within those files depends on whether they've had a background investigation or whether their personnel file——

Chairman CHAFFETZ. How many records do you have? This is what I'm trying to get at.

Ms. ARCHULETA. I'll ask Ms. Seymour.

Chairman CHAFFETZ. No, I want you. Come on, you're the head of this agency. I'm asking you, how many records are at play here?

Ms. ARCHULETA. I'll get back to you with that number, sir.

Chairman CHAFFETZ. No, no. Let me read to you what you wrote on February 2 of this year. This is to the Appropriations chairmen, both in the House and the Senate. You wrote: As a proprietor of sensitive data, including personally identifiable information for 32 million Federal employees and retirees, OPM has an obligation to maintain contemporary and robust cybersecurity controls.

You wrote that in February. Are you here to tell me that that information is all safe, or is it potentially 32 million records that are at play here?

Ms. ARCHULETA. As I mentioned to you earlier in my testimony, Mr. Chairman, we're reviewing the number and the scope of the breach and the impact to all of the records.

Chairman CHAFFETZ. So it could be as high as 32 million. Is that right?

Ms. ARCHULETA. As I mentioned to you, I will not give a number that is not completely accurate. And as I mentioned in my testimony today, I will get back to you as soon as——

Chairman CHAFFETZ. I'm asking you for a range. I don't need a specific number. We know it's a minimum of 4.2 million, but it could be as high as 32 million?

Ms. ARCHULETA. I'm not going to give you a number that I am not sure of.

Chairman CHAFFETZ. And when they fill out the SF–86, that would include other people that are identified within those forms, correct?

Ms. ARCHULETA. That's correct, sir.

Chairman CHAFFETZ. Do we know, on average, how many people are identified—if you fill out an SF–86, what's the average number of people that are identified within those records?

Ms. ARCHULETA. I don't believe anyone has calculated an average——

Chairman CHAFFETZ. Are you working on that?

Ms. ARCHULETA. As I mentioned in my testimony, each—my team——

Chairman CHAFFETZ. I'm asking you if you will take a sampling of records and understand how many other people are identified in those records. If you have 32 million employees and former employees in your database and they are also identifying other individuals, I would like to know, on average, how many people that is? Is that fair?

Ms. ARCHULETA. We're not calculating on average. We're calculating on a very distinct and accurate number. We're not going to make estimates.

Chairman CHAFFETZ. A distinct and accurate number. When you asked for $32 million more in your budget request, it was because you had 32 million Federal employees identified and former employees. Correct?

Ms. ARCHULETA. That—the number of employees that we have, yes. We're asking for support. We're asking for support for our cybersecurity——

Chairman CHAFFETZ. Ms. Seymour, do you have a complete inventory of servers, database, network, devices, and people that have access to that information? Do you have the complete inventory of that?

Ms. SEYMOUR. We have as complete an inventory as we can have, sir. That changes on a daily basis. We have run scans on our network——

Chairman CHAFFETZ. Changes on a daily basis. You either have it or you don't. You don't have it, do you?

Ms. SEYMOUR. We have an inventory of all of our——

Chairman CHAFFETZ. Is it 100 percent complete?

Ms. SEYMOUR. We believe that it is complete today.

Chairman CHAFFETZ. But the IG says that it's not complete. Mr. McFarland says that it's not complete.

Ms. SEYMOUR. His IG report was done in 2014. We've made significant progress in our IT program since then. We have tools on our network that scan our network for databases, so we know where those are, and we know the PII in them.

Chairman CHAFFETZ. To the members of the committee here, we have to move quickly, but I think just having an inventory of what's at play here is key. And the inspector general does not believe you when you say that.

Ms. Archuleta, in March of 2014, OPM became aware of an attack on its computer networks. I would highlight and I'll ask unanimous consent to enter into the record—without objection, so ordered—"Chinese Hackers Pursue Key Data on U.S. Workers." This is dated July 9 of 2014.

Chairman CHAFFETZ. As it relates to this attack, Ms. Archuleta, did it result in a breach of security?

Ms. ARCHULETA. The March 24——

Chairman CHAFFETZ. Your microphone.

Ms. ARCHULETA. On the March 2014 OPM network, the adversary activity that dated to that number was no PII was lost.

Chairman CHAFFETZ. I asked if there was a breach in security.

Ms. ARCHULETA. On March 24, there was adversarial activity that dated back to November of 2013. And with the forensics of that information, we found that no PII was lost.

Chairman CHAFFETZ. I am asking you a broader question. So did they have access to the PII, the personal identification information? Did they have access to it?

Ms. ARCHULETA. You would have to ask forensic teams. I am not a forensic expert. But we have the forensic team right here with us on this panel.

Chairman CHAFFETZ. In your perception, from your understanding, did they have access to the personal information?

Ms. ARCHULETA. We know that there is adversarial activity that dated back to November 2013. I also know that no PII was lost.

Chairman CHAFFETZ. No. That's a different question. The question I asked is, did they have access? Whether they exfiltrated it is a different question. I am asking if they had access. And I believe the answer is yes, isn't it?

Ms. ARCHULETA. That's what I've said to you, sir, that there was adversarial activity.

Chairman CHAFFETZ. So they had access to that information.

Ms. ARCHULETA. There was adversarial access, activity.

Chairman CHAFFETZ. Yes. Did it result in a breach of security, in your opinion? Is that a breach of security?

Ms. ARCHULETA. That's a breach of our systems, yes.

Chairman CHAFFETZ. Is that a breach of your security?

Ms. ARCHULETA. With the security systems, yes.

Chairman CHAFFETZ. So, yes, it was a breach of security, yes?

Ms. ARCHULETA. They were able to enter our systems. The security tools that we had in place at that time were not sufficient to fight back, and we have since instituted more. And that is why, in April of this year, we were able to——

Chairman CHAFFETZ. Okay. But at the time—at the time—it was a breach of security, right?

Ms. ARCHULETA. Yes, there was a breach into our system.

Chairman CHAFFETZ. Was there any information lost?

Ms. ARCHULETA. As I have just said to you, there was no PII lost.

Chairman CHAFFETZ. That's not what I asked you. I asked, did you lose any information?

Ms. ARCHULETA. You would have to ask the forensic team.

Chairman CHAFFETZ. I am asking you if any information was lost.

Ms. ARCHULETA. I will get back to you with that answer, sir.

Chairman CHAFFETZ. I believe you know the answer to this question.

Ms. ARCHULETA. You believe I know the answer to this question?

Chairman CHAFFETZ. Yes. Did they take any information when they hacked into the computers?

Ms. ARCHULETA. I have been advised by my CIO and our forensic team that no PII was lost.

Chairman CHAFFETZ. That's not what I asked you. We will take as long as you want here. I did not ask if they just exfiltrated PII. I am asking you, did they take any other information?

Ms. ARCHULETA. I will get back to you.

Chairman CHAFFETZ. I know you know the answer to this question.

Ms. Seymour, did they take any other information?

Ms. SEYMOUR. In the March 2014 incident, the adversaries did not have access to data on our network. They did have access to some documents, and they did take some documents from the network.

Chairman CHAFFETZ. What were those documents?

Ms. SEYMOUR. Those documents were some outdated security documents about our systems and some manuals about our systems.

Chairman CHAFFETZ. What kind of manuals?

Ms. SEYMOUR. Manuals about the servers and the environment.

Chairman CHAFFETZ. Is it fair to say—is that like a blueprint for the system?

Ms. SEYMOUR. It would be fair to say that that would give you enough information that you could learn about the platform, the infrastructure of our system, yes.

Chairman CHAFFETZ. Did they take any personnel manuals?

Ms. SEYMOUR. No, sir, they did not take——

Chairman CHAFFETZ. But they——

Ms. SEYMOUR. They took some manuals about the way that we do business. They didn't take personnel manuals. I am not—we may be not defining that the same way.

Chairman CHAFFETZ. But they did take information.

Ms. SEYMOUR. Yes, sir, they did.

Chairman CHAFFETZ. Do you believe it was a breach of security?

Ms. SEYMOUR. Yes, sir, I do.

Chairman CHAFFETZ. So, Ms. Archuleta, when we rewind the tape and look at the WJLA–TV interview that you did on July 21, you said: Again, we did not have a breach in security. There was no information that was lost. That was false, wasn't it?

Ms. ARCHULETA. I was referring to PII.

Chairman CHAFFETZ. No, you weren't. That wasn't the question. That was not the question. You said, "There was no information that was lost." Is that accurate or inaccurate?

Ms. ARCHULETA. The understanding that I had of that question at that time referred to PII.

Chairman CHAFFETZ. It was misleading. It was a lie, and it wasn't true. And when this plays out, we are going to find that this was the step that allowed them to come back and why we are in this mess today. It was not dealt with. You were misleading when you went on television and told all the employees, all these Federal employees watching local television: Don't worry, there is no information lost.

Did they have access to personnel information, Ms. Seymour?

Ms. SEYMOUR. No, sir, at that time, they did not have access to personnel information.

Chairman CHAFFETZ. They may not have exfiltrated it, but did they have access to it? Could they look at it?

Ms. SEYMOUR. No, sir, at that time, they did not have access to personnel information.

Chairman CHAFFETZ. We will explore that more. Thank the indulgence of the committee.

Now recognize Mr. Cummings.

Mr. CUMMINGS. Mr. Giannetta, I will get to you in a minute.

But I want to talk to you, Mr. McFarland. And I want you to hear me very carefully, listen to me carefully. There have been, after our last hearing on this subject, members on both sides have wanted to ask for Ms. Archuleta's resignation. And I asked that we not do that, but we have this hearing so we could clear up some things and because I wanted to make sure we were all hearing right, and we are being fair.

This is my question. You have one opinion, and Ms. Archuleta, Director Archuleta, and Ms. Seymour have another opinion. You seem to say they need to do certain things in a certain order. They say they think the order that they are doing them in is fine. They say they can do certain things in a short time. You say it's going to take longer. You also say that they don't have the necessary stream of funding that they may need.

This is what I want to know. Is this a difference of opinion with regard to experts? You understand what I am saying? You have your set of experts; they have their set. Is it a difference? Do you deem it a difference of opinion? The reason why I mention from the very beginning about the desire of certain members of our committee to ask for Ms. Archuleta's dismissal is because I want you to understand how significant that answer is because there are some members who believe that you have made recommendations and that those recommendations have been simply disregarded.

And so can you help us with that, Mr. McFarland? Do you understand my question? You look confused. Don't be confused.

Mr. MCFARLAND. I always look that way.

Mr. CUMMINGS. Oh, good. You always look that way. Okay. Go ahead.

Mr. MCFARLAND. I am not confused, no, but it is a difficult question.

Mr. CUMMINGS. But it's a very important question.

Mr. MCFARLAND. Yes, absolutely. Well, of course, it's a difference of opinion.

But the opinion that I have comes from auditors who are trained to look for the things that they reported on. And they did, in my estimation, as normal and usual, an excellent job. And they stand behind their findings. And I stand behind their findings.

Mr. CUMMINGS. But is this a difference of opinion?

Mr. MCFARLAND. Well, it's obviously a difference of opinion. But I think, without question, from my perspective, ours is based on auditing and questioning and understanding of the situation. And that's where we come up with our answer.

Mr. CUMMINGS. Let me ask you this. You heard Ms. Archuleta give a whole list of things that she is doing or about to do, I think naming a new cyber officer and whatever. Does that satisfy you as far as your concerns are involved?

Mr. MCFARLAND. Well, no, it doesn't satisfy me as far as our concerns. We have a whole suitcase of concerns that we have identified in our reports. I think that the best way to explain or answer that question is that we are, I guess, very frustrated that we ask answers of OPM, and it takes a long time to get the answers. We ask definitive questions, and we don't necessarily get definitive answers. We know for a fact that the things that we have reported

are factual. We don't take a back seat to that at all. Our people have done this for a long time. They know what they are doing.

But, yes, it comes out to a difference of opinion, but ours is based on fact. I can't speak for the other side.

Mr. CUMMINGS. All right.

Mr. Giannetta, your company, USIS, and its parent company, Altegrity, have a lot to answer. According to the Justice Department, USIS perpetrated a multimillion dollar fraud, orchestrated at the highest levels of the company. USIS failed to protect sensitive information of tens of thousands of Federal employees, including people in the intelligence community and even the Capitol Police. And Altegrity doled out millions of dollars of bonuses to top executives during the fraud and after the data breach.

I want to question you about USIS and Altegrity's pattern of refusing to cooperate with this committee and our requests for information. Last week, the committee invited Altegrity's chairman to testify. Do you know what he said?

Mr. GIANNETTA. I do not.

Mr. CUMMINGS. I will tell you. He said no. He refused.

In 2014, a team from the Department of Homeland Security asked Altegrity if they could scan the networks of Altegrity's other subsidiaries because the cyber spies were able to move from USIS to those other subsidiaries.

Mr. Giannetta, do you know how Altegrity responded?

Mr. GIANNETTA. I understand they declined the request.

Mr. CUMMINGS. Yeah, that's right. They refused. They would not allow DHS to examine the other Altegrity subsidiaries. Mr. Giannetta Altegrity is your parent company at USIS. Who at Altegrity made decision to refuse the government's requests?

Mr. GIANNETTA. I don't have that information. I am not aware who made that decision. It certainly wasn't me.

Mr. CUMMINGS. Well, can you find out for us?

Mr. GIANNETTA. I can ask.

Mr. CUMMINGS. How soon can we get that information?

Mr. GIANNETTA. I will take it back to counsel and see what we can do.

Mr. CUMMINGS. I will just ask you get it to us within the next 24 hours. I would like to have that. We have been trying to get it for a long time. I would like you to tell the committee the names of the specific members of the board who made the decision. All right?

Mr. GIANNETTA. Sir, I am the chief information officer at USIS. I interact almost never with the board of directors. I don't know——

Mr. CUMMINGS. Mr. Giannetta, you are about as close—we have been trying to get this information for a while. You are all we got. I know you are just back from vacation from Italy. Did you get a bonus, by the way?

Mr. GIANNETTA. I did.

Mr. CUMMINGS. Oh, my goodness. How much did you get?

Mr. GIANNETTA. I don't recall the exact amount.

Mr. CUMMINGS. You can tell me.

Mr. GIANNETTA. It was in the neighborhood of $95,000.

Mr. CUMMINGS. All right. Your company also refused to provide answers to questions that I asked at a hearing in February 2014 and again by committee letter, dated March 18, 2014. Mr. Giannetta, do you know what your company representatives said when the committee attempted to get these answers?

Mr. GIANNETTA. I am not in that communication chain, so I don't.

Mr. CUMMINGS. Let me tell you. They sent an email sent to our committee staff, and Altegrity's attorney wrote, "The company does not anticipate making a further response." Would you know why they would say that?

Mr. GIANNETTA. Again, I am the chief information officer at USIS. I really don't know.

Mr. CUMMINGS. It sounds pretty arrogant to me. So let me ask you right now the same question I asked back in February of 2014, more than 16 months ago. Name the members of Altegrity's board of directors who decided not to answer those questions. You wouldn't know that either.

Mr. GIANNETTA. I don't know the board of directors. I know the chairman's name is Steve Alesio. I don't anybody else at the board. I apologize.

Mr. CUMMINGS. So you are still working for USIS. Is that right?

Mr. GIANNETTA. That's correct.

Mr. CUMMINGS. How long will you be there?

Mr. GIANNETTA. Indeterminate, but within the next month or so, I will be departing.

Mr. CUMMINGS. And will you try to get me those names?

Mr. GIANNETTA. I will certainly take your request back to the appropriate people.

Mr. CUMMINGS. All right.

Thank you very much, Mr. Chairman.

Chairman CHAFFETZ. I will now recognize the gentleman from Florida, Mr. Mica.

Mr. MICA. Thank you, Mr. Chairman.

And, Ms. Archuleta, there has been a discussion today about how many people's—Federal employees' and retirees'—records have been breached. And you testified at the beginning you estimated about 2.4 million. Was that correct?

Ms. ARCHULETA. No, in the personnel records, it was 4.2. And we haven't given an estimate for the second incident.

Mr. MICA. 4.2 in personnel. Because half of that is retirees, is that 2.4, and then you add the other balance?

Ms. ARCHULETA. I don't know exact percentage, but it's about half and half.

Mr. MICA. Okay. Then the second figure you started to debate a bit about was 18 million, which has been reported by the media, but—and that would deal with breach of Social Security numbers?

Ms. ARCHULETA. The analysis right now is taking a look at all the PII because PII comes in various forms. It could be a Social Security number.

Mr. MICA. But you are not prepared to tell us how many of the Social Security numbers are breached.

Ms. ARCHULETA. No, sir.

Mr. MICA. And then the chairman pointed out your statement, I guess it was in February, that you had, say, over 32 million records.

Ms. ARCHULETA. That was a number he used, yes.

Mr. MICA. You really don't know then how many records have been breached beyond the 4.2?

Ms. ARCHULETA. No, sir. That's the investigation we are doing right now.

Mr. MICA. You know, I thought about this a little bit. And I thought, well, first thing, were my records breached, my staff, and others? And then I was thinking of people downtown that work in the agencies. And we have an important responsibility to protect the information, their personal information. Over the weekend, in fact Monday, I spent at one of our embassies overseas being briefed all morning on a bunch of issues. And brought to my attention by some of the people serving in some sensitive positions were that they were notified by you all of a breach of their records. So our overseas personnel in sensitive positions have also been subject to this breach. Is that correct?

Ms. ARCHULETA. Employee personnel records on current employees who have records at OPM have been——

Mr. MICA. How much data? Is their address? But there is personal information about these individuals. You know, you think a little bit about people down in the glass places here, you want everyone safe. I was absolutely stunned to find out that some of the people, United States citizens serving overseas, were notified that their personnel records have been breached, and information is available on them, and they are in possible situations that could be compromised by that information. But you have notified them, right?

Ms. ARCHULETA. We have notified the 4.2 million people.

Mr. MICA. Those are the people. They mentioned this to me. I was there on other subjects but expressed concern.

Ms. ARCHULETA. And I am as concerned as you are, sir, about this because these are the individuals who have been—whose data has been taken by these attackers. I am as concerned as you are.

Mr. MICA. These people are on the front lines overseas, and they are representing us. And I could hear concern in their voice about what's been—what has taken place. I read—is it Chinese hackers? Does anyone know? Was it Chinese? Do we know for sure? Do you know for sure?

Ms. ARCHULETA. That's classified information, sir.

Mr. MICA. So you have some idea, but it's classified?

Ms. ARCHULETA. That's classified information. I can't comment. I would be glad to in another——

Mr. MICA. Okay. Now whether it's Chinese or some group that could give this information to people who would want to do harm, that means some of those people to me are at risk.

Ms. ARCHULETA. Sir, every employee is important to me, not whether they are serving in Kansas City or they are serving overseas. Every employee is important to me.

Mr. MICA. Yesterday morning before I left, I visited a site of a terrorist act in one of the capitals. And I saw that—well, that place still hasn't been opened, and it has been months since that ter-

rorist attack. And our people are over there on the front lines and, their information has been compromised.

Now, you have been there the longest, Ms. Barron-DiCamillo, is that the truth? I mean, since about 2012, is it?

Ms. BARRON-DICAMILLO. I am sorry, what was——

Mr. MICA. You have been in position since 2012 at OPM?

Ms. BARRON-DICAMILLO. No, I work for Department of Homeland Security.

Mr. MICA. Homeland Security, I am sorry, but you are responsible overseeing OPM's——

Ms. BARRON-DICAMILLO. So DHS has a shared responsibility for cybersecurity. We are partnering with departments and agencies to ensure the cybersecurity of the dot-gov and working with critical infrastructure partners. And we work with them protecting at the boundaries as well as——

Mr. MICA. When did we first find out about this breach?

Ms. BARRON-DICAMILLO. It was notified by a third-party partner to us——

Mr. MICA. When? What date?

Ms. BARRON-DICAMILLO. —in March of 2014.

Mr. MICA. 2014. So when you came on, Ms. Seymour, about 2014?

Ms. SEYMOUR. I came on board in December of 2013, sir.

Mr. MICA. 2013, so you were there. They talked about his bonus. Finally, are you SES?

Ms. SEYMOUR. Yes, sir, I am.

Mr. MICA. Did you get a bonus too?

Ms. SEYMOUR. Yes, sir, I did.

Mr. MICA. How much?

Ms. SEYMOUR. I do not know the exact amount, but I believe it was about $7,000.

Mr. MICA. Okay. So whether you were private or public, people were getting bonus while some of this was going on.

Thank you, Mr. Chairman.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentlewoman from New York, Mrs. Maloney, for 5 minutes.

Mrs. MALONEY. Thank you.

I am trying to get this straight. OPM was breached directly. Is that correct? And I am going to ask Ms. Seymour, the information officer. OPM was breached twice directly. Is that correct?

Ms. SEYMOUR. Yes, ma'am, that's correct.

Mrs. MALONEY. And one was in—one occurred in December of 2014, detected in April 2015. And then the security breach—when were the two breaches? When were the two breaches? The dates?

Ms. SEYMOUR. The first OPM breach goes back to we discovered it in March of 2014, and the breach actually—the breach actually occurred in——

Mrs. MALONEY. You discovered it in March 2014?

Ms. SEYMOUR. Yes, ma'am. And the breach actually occurred, the adversary had access back to November of 2013.

Mrs. MALONEY. November 2013. Okay. And then the second breach was when? There were two breaches, correct?

Ms. SEYMOUR. That is correct, ma'am. The second breach we discovered in April of 2015, and the date that that breach goes back to is October of 2014—I am sorry, June of 2014.

Mrs. MALONEY. June of 2014.

Ms. SEYMOUR. Yeah.

Mrs. MALONEY. Who discovered this breach? How did OPM discover this breach?

Ms. SEYMOUR. The first breach we were alerted by DHS.

Mrs. MALONEY. So you did not discover it. The Department of Homeland Security discovered it?

Ms. SEYMOUR. The first breach in March of 2014——

Mrs. MALONEY. In 2014. Wait a minute. I think this is important. Homeland Security discovered it.

Ms. SEYMOUR. Yes, ma'am.

Mrs. MALONEY. Okay. And then the second one, who discovered it?

Ms. SEYMOUR. OPM discovered it on its own in April of 2015. By then, we had put significant security measures in our network.

Mrs. MALONEY. Now, when did you report these breaches, and who did you report them to?

Ms. SEYMOUR. On April 15, when we discovered the most recent breach, we reported that to US–CERT and to——

Mrs. MALONEY. Who?

Ms. SEYMOUR. The Computer Emergency and Readiness Team, DHS.

Mrs. MALONEY. You did it to DHS. Did you report it to Congress?

Ms. SEYMOUR. We also reported it to the FBI, and then we made our FISMA-required notification to Congress as well.

Mrs. MALONEY. Okay. That was the April 15 one. What about the first one?

Ms. SEYMOUR. For the first breach, and again DHS notified us of that activity in our network. And so they already knew about that one. And yes, ma'am, we made notifications to Congress of that one as well.

Mrs. MALONEY. When?

Ms. SEYMOUR. I am sorry, ma'am, I don't have that date in my notes. I would be happy to get you a response.

Mrs. MALONEY. Would you please get that back to the committee for us?

Mrs. MALONEY. Did you notify the contractors of the breach?

Ms. SEYMOUR. At the first breach, there was not an awareness of that—of what the adversaries were targeting and that this may go beyond OPM. I know that our staffs, my staff, my security staff had conversations with the security staffs at the contractor organizations. I also know that the indicators of compromise that DHS had were provided to other government organizations, were put into EINSTEIN, as well as they have communications that they would normally——

Mrs. MALONEY. But the breaches were direct. Now, I want to understand the interaction with the contractors. Now, when they breached you, did it go into OPM? I am asking both Mr. Hess and Mr. Giannetta. When they went into your system, did that connect into OPM, or was it held in your system?

Mr. GIANNETTA. In our intrusion in June of 2014, it was within our systems.

Mrs. MALONEY. So it was within your system. So the 4 million identities that they have and information they have, it came from OPM, or it came from the contractors? Are they one and the same, or are they separate? And I will go back to Ms. Seymour.

Ms. SEYMOUR. No, ma'am, these are separate incidents. So with the breach at USIS, the way that OPM does business with its contractors is different from the way other agencies may do business with both KeyPoint and with USIS. And so there were approximately 49,000, I believe it was, individuals who we notified based on the KeyPoint incident. There were other agencies who made notifications both on the USIS—based on the USIS and the KeyPoint incidents.

The 4.2 number that you are getting to, ma'am, is about the personnel records that are the incident at OPM.

Mrs. MALONEY. What I would like to get in writing is exactly what information came out of OPM, what information came out of the contractors. Is it the one and the same? You are the final database. So I want to understand the connection and how the breaches occurred and how they interconnected. If you could get it back to Chairman Chaffetz, I think it is important information.

Chairman CHAFFETZ. Thank you. Thank the gentlewoman.

Now recognize the gentleman from Ohio, Mr. Turner, for 5 minutes.

Mr. TURNER. Thank you, Mr. Chairman.

Ms. Archuleta and Ms. Seymour, I just want to remind you that you are under oath. And I have a series of questions that follow on to Chairman Maloney's questions.

It was reported in the Wall Street Journal that a company named CyTech has related that they were involved in discovering the breach that apparently has been, according to this article, linked to Chinese hackers. OPM's press secretary said the assertion that CyTech was somehow responsible for the discovery of the intrusion into OPM's network during a product demonstration is inaccurate. CyTech related that they were invited in by OPM, that they—Ms. Seymour? Ms. Seymour, could I have your attention? That they were invited in by OPM and that their equipment was run on OPM and that their equipment indicated that there had been an intrusion of your system, that they notified you.

But your response officially from OPM is that it's inaccurate, that they were not involved. Ms. Archuleta, I believe you were asked this question previously, were you not, and you said that they were not involved?

I remind you both that you are under oath. Anybody want to change their answer? Was CyTech involved in the discovery of this data breach? Ms. Archuleta?

Ms. ARCHULETA. No, they were not.

Mr. TURNER. Ms. Seymour?

Ms. SEYMOUR. No, sir, they were not.

Mr. TURNER. Okay. Now, reminding you again you are under oath, was CyTech ever brought in to run a scan on OPM's equipment?

Ms. SEYMOUR. CyTech was engaged with OPM, and we had—we were looking at using their tool in our network. We gave them—it is my understanding that we gave them some information to demonstrate whether their tool would find information on our network, and that—in doing so, they did indeed find those indicators on our network.

Mr. TURNER. Great. Well, thanks, Ms. Seymour. Because I sit on the Intelligence Committee. And CyTech Services president and CEO, Ben Cotton, and his vice president of technology development, John Irvine, came in and briefed the Intelligence Committee staff. And they relate that they were given access to your system, ran their processes, and their processes discovered it. And I think you are confirming this now, where previously it was denied that they had any involvement.

So you want to relate again, Ms. Seymour, what exactly did CyTech do? Were they given access to your system? Did they run it on your system?

Ms. SEYMOUR. Here is what I understand, sir. OPM discovered this activity on its own.

Mr. TURNER. That wasn't the question, Ms. Seymour. And I am assuming that you would have greater than an understanding, that you would actually know, considering you are the chief information officer, and you are testifying before us as to how this happened, and there has already been a news article on this. So please tell us clearly what access was CyTech given to your system.

Ms. SEYMOUR. I will be happy to answer your question, sir. I am trying to explain to you how CyTech had access. OPM discovered the breach, and we were doing market research, and we were also—we had purchased some licenses for CyTech's tool. We wanted to see if that tool set would also discover what we had already discovered. So, yes, they put their tools on our network, and yes, they found that information as well.

Mr. TURNER. So you were tricking them? You like already knew this, but you brought them in and said, Shazam, you caught it too? That seems highly unlikely, don't you think?

Ms. SEYMOUR. We do a lot of research before we decide on what tools we are going to buy for our network.

Mr. TURNER. At that point you hadn't removed the system from your system? I mean, you knew it was there, you brought them in, and their system discovered it too, which means it would have to have been continuously running, and that personnel information would have been still at risk.

Correct?

Ms. SEYMOUR. No, sir. We had latent malware on our system that we were watching that we had quarantined.

Mr. TURNER. You had quarantined it. So it was no longer operating.

Ms. SEYMOUR. That is correct.

Mr. TURNER. Okay. Well, clearly, you are going to have to give us all an additional briefing and certainly the Intel Committee staff an additional briefing on exactly how you did this because, you know, CyTech's relating what they did is very compelling. And, quite frankly, what you say sounds highly suspicious, that you would have brought them in, tricked them to see if they could dis-

cover it, something you have already discovered. I mean, why would you need them if you have already discovered it? And then further tricked them to say, Well, you don't really have the system on your system anymore? It just contradicts in so many ways it defies logic.

But the other thing I want to ask you, Ms. Archuleta, is on your SF–86 forms that were compromised——

Ms. ARCHULETA. Yes.

Mr. TURNER. When you say a form, it just sounds so minor. But this is the form, this is the Security Form 86 that people looking to work on national security and get clearance have to fill out. It's not just their Social Security, but their Social Security number is all over this. What are you doing—I have Wright-Patterson Air Force Base in my district. My community has a number of people who have had to fill these out to be able to serve their country. What are you doing about the additional information that's in this form that's being released and that's out there about these individuals?

Ms. ARCHULETA. I filled out exactly the same form. And——

Mr. TURNER. I didn't ask that. I asked you, what are you doing? Because it is not about just identity theft. This is not just their credit cards and their checking accounts. What are you doing about the rest of information that is in here about counseling them and assisting them?

Ms. ARCHULETA. I just used that by way of example that I understand what is in the form, personally, and as Director of OPM and because, at OPM, as you know, we do Federal background investigations, and I am clearly aware of what is in the form. As I mentioned in my testimony, that we are working with a very dedicated team to determine what information was taken from those forms and how we can begin to notify the individuals who were affected by that. That form is very complicated. And that is why I am very, very careful about not putting out a number that would be inaccurate. That is a complicated form, with much information. It has PII and other information. So we want to be sure that as we look at how we protect the individuals who completed those forms that we are doing everything we can. We are looking at a wide range of options to do that.

This is an effort that was working on together throughout government, not just OPM. We are all concerned about the data that was lost as a result of this breach by these hackers who were able to come into our systems. And I will repeat again, but for the fact that we found this, this malware would still be in our systems.

Mr. TURNER. Mr. Chairman, I just want to thank them for at least acknowledging that CyTech had access to their equipment and that did run and did identify this, even though they previously denied CyTech's involvement. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentlewoman from the District of Columbia, Ms. Norton, for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman.

Actually, I have a question for Ms. Barron-DiCamillo.

But, first, I want to ask Ms. Archuleta, members have been concerned about this 4.2 million number. You have tried to straighten

that out. For the record, that is not a final number. It almost surely will go up. Is that the case?

Ms. ARCHULETA. There are two incidents.

Ms. NORTON. I understand that.

Ms. ARCHULETA. So, in the first incident, that number is 4.2 million. In the second incident, we have not reached a number.

Ms. NORTON. So the number is going to go up. I understand—indeed, I am receiving calls from Federal employees about OPM's promise of 18 months, I believe it is, free credit monitoring. Is it true that Federal employees must pay for this service——

Ms. ARCHULETA. No.

Ms. NORTON. —after that time?

Ms. ARCHULETA. The service—well, the services that we are offering is identity theft protection up to a million dollars. We are also offering credit monitoring for 18 months, which is the standard industry practice. As we look at the second notification, we are looking at our whole range of options.

Ms. NORTON. Ms. Archuleta, there is a great deal of concern, not so much about how much to pay for it but the amount of time, that the 18 months may be too short a period of time given how much you don't know and we don't know.

Ms. ARCHULETA. And we are getting tremendous information back from not only——

Ms. NORTON. Well, are you prepared to extend that time if necessary?

Ms. ARCHULETA. I have asked my experts to include this feedback that we have received on a number of different considerations that need to be made.

Ms. NORTON. I will ask, are you prepared to extend that 18 months in light of what has happened to Federal employees if necessary?

Ms. ARCHULETA. As I said, we don't know the scope of the impact of the—the scope of——

Ms. NORTON. Precisely for that reason, Ms. Archuleta, I have got to go on. If the scope is greater as you get more information, will you correlate that to extending the amount of time that Federal employees have for this credit monitoring?

Ms. ARCHULETA. Congresswoman, I will get back with you as to how and what range of options we have.

Ms. NORTON. Will you get back to us within 2 weeks on that?

Ms. Archuleta, we have people out there, all of us have constituents out there who have been directly affected. When you won't even tell me that you are prepared to extend the time for credit monitoring, what kind of satisfaction can they get from OPM? I am just asking you that if necessary——

Ms. ARCHULETA. Congresswoman, I am as concerned as you are.

Ms. NORTON. In other words, you are not even willing to answer that question. Are you willing to answer this question: They report having to wait long periods of time, sometimes hours, to even get anybody on the phone from OPM. Can you assure me that if a Federal employee calls they can get a direct answer forthwith today if they call? And if not, what are you going to do about it?

Ms. ARCHULETA. We are already taking steps. And what the contractor has actually implemented is a system similar to what the

Social Security is using. So if they get a busy tone, they also can leave their number, and they will get a call back.

Ms. NORTON. Within what period of time, Ms. Archuleta?

Ms. ARCHULETA. For example, I have heard a gentleman told me this morning that he left his number, and he was called back in an hour. So that individual does not have to wait on the phone. It is a very simple process.

Ms. NORTON. Ms. Archuleta, you let the chairman know before the end of this week what is the wait time for a return call.

Ms. ARCHULETA. Yes.

Ms. NORTON. That was a subject of great concern.

Ms. ARCHULETA. I would be glad do that. We get those numbers every day. I would be glad do that.

Ms. NORTON. We need to do all we can to give some assurance. We can't even assure them that beyond 18 months, they are going to get credit monitoring. That's a very unsatisfactory answer, I want you to know.

I want to ask Ms. Barron-DiCamillo, we understand that much of this is classified, and we keep hearing: We can't tell you things because it's classified.

Of course, the press is finding out lots of stuff. They reported that law enforcement authorities have been examining the connection between the cyber attack at OPM and a previous data breach that occurred at KeyPoint. So I want to ask you, Ms. Barron-DiCamillo, and I don't want to discuss—I am not asking about anything classified—in the course of your own investigation at US–CERT into KeyPoint's data breach, did you find that hackers were able to move around the company network prior to detection?

Ms. BARRON-DICAMILLO. In the case of the KeyPoint investigation?

Ms. NORTON. Yes.

Ms. BARRON-DICAMILLO. Yes, ma'am, they were able to move around in the KeyPoint network. We had an interagency response team that spent time reviewing the KeyPoint network after a request for technical assistance.

Ms. NORTON. Even to the domain level?

Ms. BARRON-DICAMILLO. Correct. They had access to—we were there in August of 2014. The onsite assistance team was able to discover that they had access——

Ms. NORTON. What does that allow hacker to do if you can get to the domain level?

Ms. BARRON-DICAMILLO. Well, they had access to the network since——

Ms. NORTON. KeyPoint.

Ms. BARRON-DICAMILLO. Yeah, KeyPoint network, from that point in time through the fall of 2013. So, during that time, they were able to leverage certain malware to escalate privileges for the entry points. So they entered the network, we are not quite sure how. Because of a lack of login, we couldn't find the——

Ms. NORTON. But they could get the background checks on Federal——

Mr. WALBERG. [Presiding.] The gentlelady's time has expired.

Ms. NORTON. I just want to get to this final thing. They could get the background checks on Federal employees.

Ms. BARRON-DICAMILLO. No, they could not. They were not able to—there was no—or there was a PII loss associated with 27,000 individuals associated with that case, I believe. But it was potentially exposed. Because of a lack of evidence, we weren't able to confirm that. So they had potential access, but we weren't able to confirm exfiltration of that data.

Mr. WALBERG. I thank the gentlelady.

Ms. NORTON. Thank you, Mr. Chairman.

Mr. WALBERG. I now recognize myself for 5 minutes of questioning.

Let me ask Ms. Archuleta, what do you believe was the intent behind the attack? We are talking all about the attack. So what do you think the intent was?

Ms. ARCHULETA. You would have to ask my partners in cybersecurity about that. I am not an expert in what the——

Mr. WALBERG. Ms. Seymour, maybe you could respond?

Ms. ARCHULETA. I think that may be better placed with DHS and perhaps others.

Mr. WALBERG. Let me start, Ms. Seymour, do you have any idea as to why the attack?

Ms. SEYMOUR. OPM does not account for attribution or the purpose to which this data would be used.

Mr. WALBERG. Ms. Barron-DiCamillo?

Ms. BARRON-DICAMILLO. I would be happy to discuss those types of issues further in a closed setting, as we did yesterday with the staff, because the details around that is something that would be more appropriate for a closed classified setting.

Mr. WALBERG. Ms. Archuleta, how would you assess OPM's communication with current and former Federal employees regarding the breach?

Ms. ARCHULETA. I believe——

Mr. WALBERG. At this point in time, how would you assess it?

Ms. ARCHULETA. I believe that we are very—we want to work very hard with our contractor to make sure that we are delivering the service that we want. We have asked them throughout this process to make improvements. We have demanded improvements. We are holding them accountable to deliver the services we contracted for. Ms. Seymour is in communications with them.

I do not, I do not want our employees to sit and wait on the phone. I do not want them to have to wonder whether their data has been breached. I want to serve them in every way that we can. And that is why we are demanding from our contractor the services that the contractor said they would deliver. And we are working very hard on that and each day give them the appropriate feedback from what we are hearing from our employees.

Mr. WALBERG. Federal News Radio conducted an online survey about the data breach. You probably are aware of this. One of the questions asked respondents was to rate OPM's communication with current and former Federal employees about the data breach. The results showed that 78 percent of the respondents rated that OPM's communication as poor. An additional 12 percent rated it as fair. Only 3 percent described it as good. And less than 1 percent said it was excellent. I appreciate the fact that you want to im-

prove that. We expect you to make sure that who you have contracted with improves that.

Ms. ARCHULETA. Those numbers don't make me happy, sir. And I am going do everything I can to make sure that we are doing everything for our employees. I care deeply about our employees.

Mr. WALBERG. Let me move on.

Ms. Barron-DiCamillo, some news reports indicate that attackers may now be in possession of the personal file of every Federal employee, every Federal retiree, and up to 1 million former Federal employees. If true, that means the hackers have every affected person's Social Security number, address, date of birth, job and pay history, and more that could be there. For years we have been hearing about the risk of a cyber Pearl Harbor. Is this a cyber Pearl Harbor?

Ms. BARRON-DICAMILLO. The impact associated with the data breach that was confirmed, the records that were taken out of the personal records is what we would call on a severity scale a significant impact.

Mr. WALBERG. Significant impact. What does "significant impact" mean?

Ms. BARRON-DICAMILLO. Meaning that the data, if it was correlated with other data sources, could be severely—it could impact the environment as well as the individual.

Mr. WALBERG. The "environment" meaning?

Ms. BARRON-DICAMILLO. The fact that they were able to take the data out of the environment, that's a significant impact to the environment, and ensuring that they are able to mitigate the ability that the attacker used to get into that environment. And then the fact that that data was exfilled is also considered to be a high significant impact.

Mr. WALBERG. So it's blown up.

Ms. BARRON-DICAMILLO. I am sorry?

Mr. WALBERG. It's blown up a lot of things, protection, security. It's a Pearl Harbor.

Ms. BARRON-DICAMILLO. That's not a term I am comfortable with using, but on the severity scale that we use——

Mr. WALBERG. It's pretty significant.

Ms. BARRON-DICAMILLO. Yeah. It would be medium to high significance, yes.

Mr. WALBERG. Let me ask, Ms. Seymour, do you think issuing a request for quotes on May 28 and establishing a deadline of May 29 to potential contractors was a reasonable opportunity to respond in this significant issue of cybersecurity?

Ms. SEYMOUR. Our goal was to be able to notify individuals as quickly as possible. And so we worked with the GSA schedule. We contacted schedule holders. We also put it on FedBizOpps for other opportunities. We received quotes from both schedule holders as well as nonschedule holders. And so our goal was to make sure that we could notify individuals as quickly as possible.

Mr. WALBERG. That was quick. Maybe too quick. My time has expired.

I now recognize the gentleman from Massachusetts, Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

And, again, I want to thank the witnesses for participating today.

Ms. Archuleta, you testified before the Senate. Let me ask you at the outset, who is ultimately responsible for protecting the personal identification information of employees at OPM? Or that are covered by OPM, Federal employees.

Ms. ARCHULETA. Yes, the responsibility of the records is with me and my CIO.

Mr. LYNCH. Okay. So you also testified that no one was to blame. Is that right?

Ms. ARCHULETA. I think my full statement, sir, was that I believe that the breach was caused by a very dedicated, a very focused actor who has spent much funds to get into our systems. And I have worked—the rest of my testimony was I have worked since day one to improve legacy systems.

Mr. LYNCH. I understand that. I understand that. You are blaming the perpetrators, that those are the people that are responsible. Is that basically what you are saying?

Ms. ARCHULETA. The action was caused by a very focused, aggressive perpetrator.

Mr. LYNCH. Okay. I can't have repeated the same answers.

Let me just, Mr. McFarland, the assistant inspector general, Michael Esser, testified that a number of the systems that were hacked were not older legacy systems, but they were newer systems. Is that your understanding?

Mr. MCFARLAND. Yes.

Mr. LYNCH. So this isn't the old stuff, this is the new stuff.

Mr. MCFARLAND. Yes, that's correct.

Mr. LYNCH. Okay. And the former chief technology officer at the IRS and the Department of Homeland Security said that the breaches were found bound to happen given OPM's failure to update its cybersecurity. Is that your assessment, Mr. McFarland?

Mr. MCFARLAND. Well, I think, without question, it exacerbated the possibility, yes.

Mr. LYNCH. Yeah. He also, this is a quote, he said: "If I had walked in there as the chief information officer and I saw the lack of protection for very sensitive data, the first thing we would have been working on is how to protect that data."

I am concerned as well about the flash audit that you just put out. And your ultimate determination was that you believed that what they are doing will fail.

Mr. MCFARLAND. The approach that they are taking I believe will fail.

Mr. LYNCH. Okay.

Mr. MCFARLAND. They are going too fast. They are not doing the basics. And if that's the case, then we are going to have a lot of problems down the road.

Mr. LYNCH. Let me ask you, so very crudely describing this, they are creating a shell, a protective shell. And then we're going to migrate applications in under the shell. And because they will be under the shell, they'll be resistant or impervious to hacking. It doesn't seem like we should have to wait until the last application is under the shell before we find out whether or not the shell is

working. Will that give us an opportunity to look at the early stages of this project?

Mr. MCFARLAND. Well, I am not sure if it will give us that opportunity or not. What is important, I think from our perspective, is that they have the opportunity, OPM has the opportunity right now to do certain things that will increase the security a great deal. And that shouldn't be abandoned and just placed in place of. And I don't mean to imply it is abandoned, but it should not be in place of speeding through the rest of the project to get it done. The crisis part—may not seem this way to a lot of people, but the actual crisis at OPM was with the breach. That part is over. The best thing to do is safeguard the system as it is right now and then move appropriately for a full restructuring.

Mr. LYNCH. Okay. Do you think that OPM's estimates of $93 million is accurate?

Mr. MCFARLAND. I don't think it's anywhere close to accurate.

Mr. LYNCH. I don't either. It doesn't seem to include the whole migration function where they pull the information in.

Mr. MCFARLAND. As an example, the financial system that we have, CBIS, in 2009, we had to migrate that information.

Mr. LYNCH. Right.

Mr. MCFARLAND. And in so doing, it had a lot of oversight and went pretty well. And, in fact, our office was part of that oversight. But just that one system took 2 years and $30 million.

Mr. LYNCH. Right. And that's a small fraction of what we are talking about here, right? A very small fraction.

Mr. MCFARLAND. Very small.

Mr. LYNCH. Okay.

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

Chairman CHAFFETZ. [presiding.] I thank the gentleman.

I now recognize the gentleman from South Carolina, Mr. Gowdy, for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Mr. Chairman, I want to read a regulation. I would ask all the panelists to pay attention. It's a little tedious, but it's important: If new or unanticipated threats or hazards are discovered by either the government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

That's a regulation. Mr. Hess, Mr. Giannetta, were there also contractual obligations in this realm between you and the government?

Mr. HESS. There are.

Mr. GOWDY. And they would be what, similar to that, notice? A notice provision?

Mr. HESS. I don't have an immediate recollection of exact text, but it is similarly worded.

Mr. GOWDY. Okay. I think it's helpful sometimes to define terms, particularly for those of us that are liberal arts majors and don't deal with this. What is a "new or unanticipated threat or hazard"? Mr. Hess?

Mr. HESS. That would be an indication of compromise of a system or a failure of any of the system protections.

Mr. GOWDY. Oh. So when Chairman Chaffetz was having a difficult time getting answers to that question because the focus was on the loss of personal information, that's really not what that phrase means. It's just a threat or hazard. It doesn't actually have to be a loss, does it?

Mr. HESS. Not the way I would define it.

Mr. GOWDY. Me either.

What about "existing safeguards have ceased to function?" What does that mean? Mr. Hess?

Mr. HESS. Sir, it's pretty explanatory.

Mr. GOWDY. It did strike me as being self-explanatory. It did.

Mr. Giannetta, is that self-explanatory to you, "existing safeguards have ceased to function?"

Mr. GIANNETTA. Yes.

Mr. GOWDY. Here is the really tough question, and I will let both of you weigh in on this one because it is tough. What does the word "immediately" mean?

Mr. HESS. Without delay.

Mr. GOWDY. Without delay.

Mr. Giannetta, is there another meaning that you are familiar with?

Mr. GIANNETTA. I think that's a good definition.

Mr. GOWDY. All right. So you had both a contractual obligation with the government and there is a regulatory obligation that if new or unanticipated threats or hazards are discovered by either the government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

Ms. Archuleta, I have heard this morning about a March 2014 data breach. Did I hear that right?

Ms. ARCHULETA. Yes, sir, you did.

Mr. GOWDY. And when did you bring that breach to the attention of either Mr. Hess or Mr. Giannetta? And you are welcome to turn on your microphone or else bring it closer to you.

Ms. ARCHULETA. I would have to get that information back to you. I don't have it in my notes. Perhaps Ms. Seymour would know. But if not, we would get that information back to you.

Mr. GOWDY. Do you know if it was immediately?

Ms. ARCHULETA. I would expect that it was immediate, yes.

Mr. GOWDY. Let's find out. Ms. Seymour, do you know?

Ms. SEYMOUR. No, sir, I don't. But I don't think that we—I certainly don't think that we immediately notified our contractors of a breach to our network because at that time we did not have any question as to whether it was affecting them. It was to our network at that time.

Mr. GOWDY. Mr. Hess, Mr. Giannetta, is that your understanding, that they were under no duty to bring that to your attention? Not all at once. It's your contractual language, and you are looking at the regulation. Do you think you should have been notified because of the March breach?

Mr. GIANNETTA. Absolutely.

Mr. GOWDY. Well, why? Because I just heard one person say she didn't know and the other say it was really none of your business. So why should you have been notified? Despite the plain language

of the regulation and the contractual language, why do you think it was important that you be notified?

Mr. GIANNETTA. So that we could take appropriate or more appropriate actions to protect data.

Mr. GOWDY. Were you notified?

Mr. GIANNETTA. I was not.

Mr. GOWDY. Were you notified immediately?

Mr. GIANNETTA. No.

Mr. GOWDY. Huh. What do you have to say about that, Ms. Seymour?

Ms. SEYMOUR. I believe that that's accurate, sir.

Mr. GOWDY. I am with you there. I guess my question is, why? Why, despite the plain language of the contract and the plain language of the regulation, why did you not immediately notify the contractors?

Ms. SEYMOUR. We worked with DHS and partners to understand the potential compromise to our system so that we could——

Mr. GOWDY. Was DHS one of your contractors?

Ms. SEYMOUR. No, sir.

Mr. GOWDY. Well, I didn't think so. Which that doesn't really help me understand the regulation because it says "contractor;" it doesn't say "DHS." So why didn't you notify the contractor?

Ms. SEYMOUR. At that time, we were still investigating what had happened in our network.

Mr. GOWDY. What does the word "immediately" mean to you?

Ms. SEYMOUR. Without undue delay.

Mr. GOWDY. Did you do so?

Ms. SEYMOUR. No, sir, we did not.

Mr. GOWDY. Does the regulation say "as soon as you figure out what happened" or "after you talk to DHS?" That is not in my version of the regulation. Is it in yours?

Ms. SEYMOUR. I have not read that regulation, sir.

Mr. GOWDY. You know why you haven't? Because that one doesn't exist. The one that says "notify DHS" or "try to figure it out." The only one that exists says to immediately notify the contractor, and you are telling me you didn't do it. And my question is, why?

Ms. SEYMOUR. I can't answer that question.

Mr. GOWDY. Who can?

Ms. SEYMOUR. I will take that back and get you——

Mr. GOWDY. To whom will you take it?

Ms. SEYMOUR. I believe—I would take it back to my staff to see if we have processes in place that——

Mr. GOWDY. Do you think it's staff's responsibility to notify the contractor?

Ms. SEYMOUR. We have processes in place for making notifications when we find these things.

Mr. GOWDY. Who is ultimately responsible for that process? Who failed to meet the contractual and regulatory obligations?

Ms. SEYMOUR. I would have to read that regulation, sir. I am not familiar with it.

Mr. GOWDY. I just read it.

Ms. SEYMOUR. I would be happy to read it. I would like to read the full context of it.

Mr. GOWDY. You think the context is different from what I just read?

Ms. SEYMOUR. I would want to read the context and——

Mr. GOWDY. How about the contract? Have you read the contract?

Ms. SEYMOUR. I have read most of the parts of the contract, sir.

Mr. GOWDY. Well, I can't speak for the chairman, but my guess is that he and the other members would be really interested in who failed to honor both the letter and the spirit of the contractual obligation and the regulatory obligation.

With that, I will yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the gentleman from California, Mr. Lieu, for 5 minutes.

Mr. LIEU. Thank you, Mr. Chairman.

I have concerns not just about the failures of OPM leadership but also the failures of its contractors, in particular USIS, because it looks like what happened here wasn't just recklessness or negligence; it was fraud. And I want to know how far up this fraud went. I want to know if the parent company knew about it. I want to know if the hedge fund managers that funded these companies knew about it.

So let me begin with Mr. McFarland. As you know, the Department of Justice joined a lawsuit against USIS in January for defrauding the government under its contract with OPM. And according to Justice Department filing, "Beginning in at least March 2008 and continuing for through at least September 2012, USIS management devised and executed a scheme to deliberately circumvent contractually required quality reviews of completed background investigations in order to increase the company's revenues and profits." You assisted their investigation in this case, correct?

Mr. MCFARLAND. That's correct.

Mr. LIEU. As I understand it, the parent company, Altegrity, paid bonuses to top executives at USIS during the period of their fraud that amounted to about $30 million.

Mr. McFarland, to your knowledge has USIS or Altegrity paid the government back for those bonuses?

Mr. MCFARLAND. I am not positive, but I believe not.

Mr. LIEU. All right. Let me enter into the record, Mr. Chairman, if possible, an article from the Wall Street Journal entitled "Altegrity Executives Got Pay Out Before Screener Went Bankrupt."

Chairman CHAFFETZ. Pardon me.

Mr. LIEU. If I could enter an article into the record.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LIEU. Thank you.

I ask a second one to be entered, which is an article from The Washington Post. It states that the Justice Department filed a motion in this case on Friday in U.S. bankruptcy court, seeking $44 million from USIS' parent company, Altegrity. That is from this Monday.

If we could enter that, as well.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LIEU. Okay.

Now, let me ask Ms. Barron-DiCamillo: For USIS to have upgraded assistance to prevent these kinds of breaches, it would have cost well less than $30 million; isn't that correct?

Ms. BARRON-DICAMILLO. So, not having investigated specifically, you know, the breadth and depth of all of the parent companies as well as subsidiaries—we were focused just on the USIS network—the findings estimates were actually higher than $30 million for the recommendations that we had provided to them at the end of our assessment. And that number could be as high as $50 million.

Mr. LIEU. Got it. Thank you. I appreciate that.

So now I want to ask Mr. Giannetta about the bonuses awarded during the alleged fraud.

Who on the board reviewed the deplorable performance of the CEO and decided to award him with $1 million in bonuses during the 4–1/2 years USIS was defrauding the government? Was it the board? Who made that decision?

Mr. GIANNETTA. So my role began at USIS in August of 2013 as the chief information officer. I don't have any knowledge, direct or indirect, of who approved or disapproved——

Mr. LIEU. So you don't know if it is the parent company or the hedge fund managers? We don't know who did this?

Mr. GIANNETTA. I don't have that knowledge.

Mr. LIEU. Okay. All right.

So we are going to send you written questions after today's hearing, and I want your commitment that USIS or Altegrity will provide answers within 30 days to our questions. Will you commit to at least that?

Mr. GIANNETTA. Certainly.

Mr. LIEU. All right.

Mr. Chairman, I also think the committee should call Jeffrey Campbell, the president of Altegrity, as well.

And let me now turn to Mr. McFarland.

You issued two IG reports, one in November of 2013 and one in November of 2014, correct, on OPM?

Mr. McFarland, you issued two IG reports, dated November 2013 and November 2014?

Mr. MCFARLAND. I'm sorry. I didn't hear the very first part.

Mr. LIEU. Okay. So you issued two IG reports, dated November 2013 and November 2014, on OPM?

Mr. MCFARLAND. You're speaking on FISMA. I'm sorry.

Mr. LIEU. No, no——

Mr. MCFARLAND. Yes.

Mr. LIEU. Yeah. All right.

So these two IG reports, would you agree with me the 2014 report is quite similar to the 2013 report because OPM actually failed to implement many of your recommendations?

Mr. MCFARLAND. I think there were many carryovers, yes.

Mr. LIEU. Okay.

And would you agree with me that this isn't a difference of opinion; you actually had OPM violating standards that the administration had put in?

So, for example, in 2014, your report on page 24 says OPM was not compliant with the Office of Management and Budget Memorandum M–11–11 that required two-factor authentication. On page

12, you also said that OPM was not compliant with National Institute of Standards guidance saying that they should just do a risk assessment.

And you would agree that OPM was not following these standards, correct?

Mr. MCFARLAND. Yes.

Mr. LIEU. Okay.

Director Archuleta, do you take responsibility for not following OMB guidance as well as guidance from the National Institute of Standards, which, had you followed, could have prevented these breaches?

Ms. ARCHULETA. Well, sir, I——

Mr. LIEU. Yes or no, do you accept responsibility for those two failures?

Ms. ARCHULETA. It can't be a yes-or-no answer.

Mr. LIEU. It is a yes or no. The IG identified that—look, do you accept responsibility for not following the OMB guidance and the National Institute of Standards guidance?

Ms. ARCHULETA. I have to——

Mr. LIEU. It's just a yes or no. Either you——

Ms. ARCHULETA. I have to take——

Mr. LIEU. You don't have to accept responsibility. I just want to know if you do.

Ms. ARCHULETA. I have to take into consideration when an audit is conducted by the auditor. I have to make an informed decision about his recommendations. It's not an issue of whether I disagree with him. I want to be sure that I——

Mr. LIEU. This is not an audit. This is the OMB. It is this administration's guidance.

Ms. ARCHULETA. And we have worked very closely with OMB to make sure that we're tracking, documenting, and justifying all of our steps in this——

Mr. LIEU. All right. My time is up.

Ms. ARCHULETA. —as we move forward.

Mr. LIEU. So I take it, you actually don't take responsibility.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from North Carolina, Mr. Meadows, for 5 minutes.

Mr. MEADOWS. Thank you, Mr. Chairman.

Ms. Seymour, let me come to you, because there seems to be some conflicting information. Before this committee, on April the 22nd, you had indicated that it was the adversary's modern technology and the OPM's antiquated system that helped thwart—in your words—thwart hackers at the first OPM attack. Is that correct?

Ms. SEYMOUR. Yes, sir.

Mr. MEADOWS. Okay.

Last week, you testified repeatedly that it was the OPM's antiquated systems that were the problem and the chief reason that the system was not secure and you didn't do just the basic cybersecurity measures of encryption and network protection.

So, I guess, my question to you, Ms. Seymour: Which is it? Is it the fact that the old system helped you or the old system hurt you? Those are two conflicting pieces of testimony.

Ms. SEYMOUR. I don't believe that they're conflicting, sir.

In the first incident, the old technology thwarted the actor because they did not know what they were doing in that environment. We immediately put in place a plan to provide better security——

Mr. MEADOWS. So you caught them immediately is what you are saying?

Ms. SEYMOUR. No, sir. I said we——

Mr. MEADOWS. Well——

Ms. SEYMOUR. —immediately put in place a plan so that we could improve the security posture. What we did was we moved to build a new architecture where we could put in additional security controls.

We also, at the very same time, put security controls in our current environment.

Mr. MEADOWS. Okay.

Ms. SEYMOUR. We did not wait.

Mr. MEADOWS. Well, you say you didn't wait once you found the problem, but is there——

Ms. SEYMOUR. Sir, we didn't wait——

Mr. MEADOWS. Hold on.

Ms. SEYMOUR. —from the day that I came on board.

Mr. MEADOWS. Let me ask the question. Is there, in the security IT/cybersecurity technology chief operators, is there anyone who would apply for a job who would suggest not to do encryption of sensitive data?

Ms. SEYMOUR. Encryption is not a panacea because of——

Mr. MEADOWS. I didn't ask that. Is there anybody in your job or a similar job who would come in and say, "We are going to protect everything; let's leave it unencrypted"? Can you think of anyone? Because I have been asking all over the United States. I can't find anybody.

Ms. SEYMOUR. So I'm going to—I'm trying to explain the situation to you.

Our databases are very, very large. Our applications are not always able to work properly and encrypt and decrypt that data. So what we have done——

Mr. MEADOWS. So you are saying that this was a volume problem, not a management problem.

Ms. SEYMOUR. Well——

Mr. MEADOWS. Because you are under oath——

Ms. SEYMOUR. Yes, sir.

Mr. MEADOWS. —and that is concerning, because you are saying that you just didn't have the resources to handle the large volume of information?

Ms. SEYMOUR. It's not a resource issue. It's whether our applications are built so that they can—so that——

Mr. MEADOWS. So they are not encrypted today.

Ms. SEYMOUR. —the encryptions can be done.

Mr. MEADOWS. So they are not encrypted today?

Ms. SEYMOUR. We have purchased the toolset, sir, and we are in the process of encrypting pieces of our databases, as opposed to the entire database. We are trying to focus on the sensitive information. That allows——

Mr. MEADOWS. I agree, we need to focus on the——

Ms. SEYMOUR. —our applications to run in an operable manner.

Mr. MEADOWS. —sensitive information.

So what do we tell the millions and millions of Federal workers, that now, because their system has been breached, now you are going to encrypt it? Do you feel like you have done your job?

Ms. SEYMOUR. I do, sir.

Mr. MEADOWS. Well——

Ms. SEYMOUR. I came on board, and I recognized these issues. And I worked with Director Archuleta to put in place a plan——

Mr. MEADOWS. Okay. Well, both of you all came in——

Ms. SEYMOUR. —that would improve OPM's security posture.

Mr. MEADOWS. —in 2013. You both came in in 2013.

Ms. SEYMOUR. At the end of 2013, yes, sir.

Mr. MEADOWS. How long did it take you to buy equipment to start encrypting?

Ms. SEYMOUR. The tool——

Mr. MEADOWS. Simple answer.

Ms. SEYMOUR. June of 2014.

Mr. MEADOWS. All right. So you bought equipment in June of 2014.

Ms. SEYMOUR. Uh-huh.

Mr. MEADOWS. So when did you start encrypting?

Ms. SEYMOUR. We have a couple of databases that are encrypted already, and we are——

Mr. MEADOWS. A couple out of how many?

Ms. SEYMOUR. Sir, we have numerous databases.

Mr. MEADOWS. Well, and that is my point.

Ms. SEYMOUR. And so it takes time, and it takes resources, and we have to test before we can just——

Mr. MEADOWS. All right.

Ms. Archuleta, let me come to you. When you applied for the job and you were going through your Senate confirmation, you said that you would make IT, technology your number-one priority. Again, in this committee, you said that it was your number-one priority.

Can you explain to the Federal workers and all those that have had their personal information breached how making it your number-one priority when you were confirmed in 2013 is still to be believed? Or was it just what you said during a confirmation hearing and you really never intended to act on it?

Ms. ARCHULETA. I believe that the record will show that I have acted on it, that I am dealing with a legacy system that has been in place for 30 years, and we are working as hard as we can. In 18 months, we have made significant progress, but so have our aggressors.

Cybersecurity is an enterprise responsibility, and I am working with all of my partners across government. And I have shown that we have prioritized this even as early as 2014 and 2015 in our budgets and in the resources that we have directed towards that.

I do not take this responsibility lightly. And, as I pledged in my confirmation hearing and as I pledged to you last week and as I have pledged to you today, I take it extremely seriously. And I am as upset as you are about every employee that is impacted by this.

That is why we're dedicating resources throughout government, not just as OPM but at every level of government, to be sure that this does not occur again.

Mr. MEADOWS. All right.

Ms. ARCHULETA. We're working very hard. I am serious about it.

Mr. MEADOWS. I appreciate that.

And I appreciate the patience of the chair.

Mr. HURD. [Presiding.] Thank you, Mr. Meadows.

Now I would like to recognize my colleague from the great State of New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Thank you for your being here today. I have a couple of questions, and I would like as short an answer as possible.

So, with regard to the one breach that involved the 4.2 million employees, those are actual employees and retirees. That is a closed system. We know how many that is.

With regard to the individuals whose information was in a system because background checks were being done with them, A, we don't know how many; B, every one of those individuals didn't ultimately get a job, so we have some people's information who aren't even employed by the Federal Government.

Is that yes—is that true, Ms. Archuleta?

Ms. ARCHULETA. Yes, that's true.

Mrs. WATSON COLEMAN. Okay.

Ms. ARCHULETA. If there was a background investigation requested.

Mrs. WATSON COLEMAN. Right.

So, in that second breach of that universe that is so large, that information was breached through a breach in the security of KeyPoint? Is that true, Ms. Archuleta? Is that——

Ms. ARCHULETA. Yes.

Mrs. WATSON COLEMAN. Someone who had credentials with——

Ms. ARCHULETA. There was a credential that was used, and that was the way that they got in——

Mrs. WATSON COLEMAN. Thank you.

Ms. ARCHULETA. —from an employee of KeyPoint.

Mrs. WATSON COLEMAN. So who is trying to identify all the universe that has been compromised through the latter breach? Is it KeyPoint who is trying to clean up its mess, or is it——

Ms. ARCHULETA. No, no.

Mrs. WATSON COLEMAN. —OPM?

Ms. ARCHULETA. We have a total enterprise-wide security team, or forensic team, that is doing the forensics on this.

Mrs. WATSON COLEMAN. Okay.

So Mr. McFarland has made a number of observations and recommendations, and I believe that I was left with the feeling that he didn't believe that OPM was moving in the right direction, on the right path to get to where it needs to go. And so I was also informed that his recommendations or his findings are a result of auditors and specialists in this area.

So I have two questions for you, Ms. Archuleta. Number one is, are you using experts and the same kinds of skill sets that Mr. McFarland is using in looking at the same things that he is looking at, number one? And, number two, do you agree with his recommendations? And if not, on what areas do you disagree?

Ms. ARCHULETA. The flash audit I can just take by way of example.

And, first of all, I want to say that I respect the inspector general's diligence in overseeing this topic. And there are areas where we have areas of agreement, and there's areas that I think we need to have further conversation about.

In terms of the existing contracts and the use of full and open competition, I would like to assure the IG that the processes we used to award the already-existing contracts have been perfectly legal, and we're going to continue to ensure that our future contracts and processes entered into will also be legal.

I also understand that he's concerned about the sole-source contract of tactical and shell that he spoke about. I understand his concerns. And I would like to remind him that the contracts for migration and cleanup have not yet been awarded, and we will consult with him as we do that.

Where we don't—where we have areas that we need to consider together—and, by the way, the IG and I meet on a monthly basis, and our staffs meet on a weekly basis or at least biweekly—I look forward to discussing to him about the major IT business case so that we can figure out what the practical——

Mrs. WATSON COLEMAN. Okay.

Ms. ARCHULETA. —timeline should be.

Mrs. WATSON COLEMAN. Thank you. I kind of get the drift then.

Tell me what you think is the timeframe for the IG's office and your office—and, Mr. McFarland, you might weigh in—necessary to get to where we need to get. Not that all these things are going to be implemented, but that we agree on what needs to be done. Are we talking about 3 months from now? Thirty days from now? Six months from now? Do we have any idea?

Ms. ARCHULETA. I would ask Donna just to talk about the tactical and the shell processes that we're using. We're trying to do that as rapidly as possible so that we can move out of the legacy network.

The issue about the migration and the cleanup we'll continue to discuss, but we're trying to rapidly move towards that shell.

Mrs. WATSON COLEMAN. Do we still have contracts with KeyPoint?

Ms. ARCHULETA. Yes.

Mrs. WATSON COLEMAN. And KeyPoint—this is to Mr. Hess, I believe.

How many contracts with how many departments do you have?

Mr. HESS. Our primary contracts are through Homeland Security and OPM.

Mrs. WATSON COLEMAN. Okay. And so, are your contracts active contracts? Are they coming to an end? Or are you at the end of these contracts? What is the——

Mr. HESS. They're all active contracts.

Mrs. WATSON COLEMAN. They are all active contracts.

Mr. McFarland, should we be ceasing our relationship with KeyPoint?

Mr. MCFARLAND. Based on what I know at this point, I have no reason to believe that we should.

Mrs. WATSON COLEMAN. That we should. That we——

Mr. MCFARLAND. No. I have no reason to believe that we should cease relationship.

Mrs. WATSON COLEMAN. That we should cease.

Mr. MCFARLAND. No. That we should not cease.

Mrs. WATSON COLEMAN. Should not.

Ms. Archuleta, do you agree with that?

Ms. ARCHULETA. I do agree with that. KeyPoint has taken the steps necessary to mitigate any security questions. They have been very active in working with us on that.

Mrs. WATSON COLEMAN. So but my question is, should we cease contracting with them? Mr. McFarland says yes, and you said yes——

Ms. ARCHULETA. No. He said no.

Mrs. WATSON COLEMAN. Both of you said no. Okay.

Mr. MCFARLAND. No, I'm sorry. I said no.

Mrs. WATSON COLEMAN. Okay. I am sorry. Thank you very much.

Mr. McFarland, last question to you. What are the three important things that we need to do just to get us back on the right track, and how long do you think it should take?

And that will be the end of my questioning, Mr. Chairman. Thank you very much.

Mr. MCFARLAND. Well, I'll give you four, if I could.

First, we'd like to see the implementation of multifactor authentication using PVI cards; then develop a comprehensive inventory of information systems, servers, and databases; then further protect existing data with encryption and data-loss-prevention technique tools; and then proceed with the infrastructure overhaul with a disciplined project management approach.

And I have no idea how long that will take for a discussion.

Mrs. WATSON COLEMAN. Thank you.

Thank you very much, Mr. Chairman. I yield back.

Mr. HURD. Thank you.

And I would now like to recognize Mr. DeSantis from Florida for 5 minutes.

Mr. DESANTIS. Thank you, Mr. Chairman.

You know, this is a really, really frustrating hearing and, obviously, a colossal failure. I mean, we have a government that will tell us how much water we can have flushing in our toilets, how much corn we have to put in the gasoline we use to drive our cars and boats, and the government will tell us the type of health insurance we can and cannot buy. And yet, on the core functions of government, the things that we all need the government to do, it seems to me that it fails habitually. And this is a major example of that.

The numbers of people affected, when Ms. Archuleta talked about we don't know on the clearance side, yeah, we don't know. You know why? Because it is not just the person who filled out the form that is at risk of that. I mean, you have friends, family mem-

bers, associates, foreign nationals who you may know, who China would like to know who those foreign nationals are. So you are talking about an exponentially larger number than just simply the number of people who filled out those forms.

And yet it seems to me that we just have bureaucratic paralysis. Nobody is really accountable.

Now, Ms. Archuleta, let me ask you: Members of this committee have called upon you to resign. You have rebuffed that. Do you still believe you should remain in your position?

Ms. ARCHULETA. I am more committed than ever to serve the employees of this administration. I am working very hard, and I think——

Mr. DESANTIS. Do you accept responsibility?

Ms. ARCHULETA. I accept the responsibilities that are given to the Director of the OPM. And I have fulfilled those responsibilities by making sure that we have the right people in the right places and seeking the resources that we need to do our work and to make sure that the systems that we have in place can do the work that they're expected to do. Again, we have a legacy system that is 30 years old.

Mr. DESANTIS. So——

Ms. ARCHULETA. We have dedicated money and human resources——

Mr. DESANTIS. And I appreciate that. And I have been here for your statements, and I have heard you make that point.

Ms. ARCHULETA. Thank you, sir.

Mr. DESANTIS. But if not you, then who, if anybody, in OPM should be held accountable for this colossal failure?

Ms. ARCHULETA. I am responsible, as the Director of OPM, for a number——

Mr. DESANTIS. Is anybody going to be held responsible?

Ms. ARCHULETA. —for a number of different responsibilities. I take very seriously, as I said in my confirmation hearing and many other hearings after, including today——

Mr. DESANTIS. But what about responsibility? Because I will——

Ms. ARCHULETA. I accept——

Mr. DESANTIS. —tell you what my constituents will tell me. They will say, "Ron, we have people mess up in the government all the time, and nothing ever happens." And that is not the world that our constituents live in, where there are usually consequences.

And so you are not committing that anybody will be fired or held accountable because of this, correct?

Ms. ARCHULETA. I am committing to you that we are going to do the best job we can.

Mr. DESANTIS. Well, and I appreciate that, but that, quite frankly, is not something that I think the American people have confidence in right now, given what has happened.

Now, let me ask Ms. Barron-DiCamillo: People have been warning about the risk of a cyber Pearl Harbor. Obviously, the IG had warned OPM about vulnerabilities in their system for years and years. Does this constitute a cyber Pearl Harbor?

Ms. BARRON-DICAMILLO. That question was asked to me earlier. I don't know if you were here.

We use a severity scale, and on the severity scale, based on the impact to data, the impact to the network, and getting back to a known, good, healthy state, we would consider this to be a medium- to high-severity-level kind of an event based on the kind of data that was possibly exposed and exfilled and then the ability for the mitigations that we put in place as part of the plan that we provided to OPM post-assessment.

Mr. DESANTIS. But those are mitigations for the system itself, correct? The mitigations that you have performed don't include mitigations for any of the capabilities that some of the people whose identities may have been compromised perform on behalf of our country, correct?

Ms. BARRON-DICAMILLO. Correct. I am a technical operator in cybersecurity operations, and we're focused on helping OPM and other departments' and agencies' critical infrastructure ensure the protection of their networks.

So when we do an event like this, we provide mitigations to help them get back to a known, good, healthy state as well as prevent these kinds of things and, if they are targeted again, which a lot of times they are, helping them detect that activity quicker in the cycle so they can contain it and then clean that up.

Mr. DESANTIS. So if China gets blackmail information that they could use against people serving in our government in important positions, if China is able to identify foreign nationals, Chinese foreign nationals maybe, who are friendly with the United States and with people, there is no way you can calculate the damage that that causes, correct?

Ms. BARRON-DICAMILLO. I'm a cybersecurity operator. That's clearly a question for intelligence—the intelligence community.

Mr. DESANTIS. And I think it is a very important question. And I think the damage to this is very, very severe.

And I yield back the balance of my time.

Mr. HURD. Thank you, sir.

I would now like to recognize my colleague from Virginia, Mr. Connolly.

Mr. CONNOLLY. I thank the chairman.

And I thank my good friend from Pennsylvania, Mr. Cartwright, for allowing me to go at this moment because I have to chair a meeting at 12:30.

Let me just say, you know, I was just listening to our colleague from Florida. It is easy to make a scapegoat out of somebody or something. That isn't to absolve people of responsibility. But what we are facing is a much bigger threat than a management snafu.

We are facing a systemic, organized, financed, pernicious campaign by the Chinese Government, in the form of the People's Liberation Army, with a trained unit to penetrate weak spots in our cyber world. And that includes the Federal Government, and it may include retail and commercial enterprises, certainly banks among them.

To pretend somehow this is Ms. Archuleta's fault is to really miss the big picture and, frankly, a disservice to our country. We have a bigger threat. Whether we want to acknowledge it or not, we now are engaged in a low-level but intense new kind of cold war, a cyber war, with certain adversaries, including China and Russia.

And it is every bit as much a threat to the security and stability of this country, and we need to gird ourselves for this battle.

And it is not okay to dismiss testimony that resources were denied. This committee led the effort, and I probably cosponsored the bill, to try to modernize how we purchase and manage IT assets in the Federal Government. Is that important? Why are these people here today before us? Because it is important. And Congress has neglected it. We can't have it both ways.

So, while we certainly hold Ms. Archuleta responsible, as the head of OPM, for how they are managing this breach and we have every right to question why the breach occurred, to make a scapegoat in this "Alice in Wonderland," you know, world we have created here sometimes, where the answer is, "Off with your head," how easy. What a cheap headline that gets. And it does get a headline every time. But it begs the question which is far more fundamental, far more profound, and far more disturbing as a threat. And that is ultimately what we need to deal with, it seems to me.

Mr. McFarland, last week, your office issued a flash audit alert to raise awareness of serious concerns over OPM's ongoing overhaul of its entire IT infrastructure. According to that flash alert, your office stated, "In our opinion, the project management approach for this major infrastructure overhaul is entirely inadequate and introduces a very high risk of project failure."

If I understand correctly, what you are saying is that the project won't do what we need it to do. Is that correct, Mr. McFarland?

Mr. MCFARLAND. No, I'm not saying that the project wouldn't ultimately do what is hoped for. I'm saying that the potential for problems exists, and it is very high probability——

Mr. CONNOLLY. Well, I want to use the word in the report: "entirely inadequate"; "introduces a very high risk of project failure." That doesn't say, to me, there is the possibility of failure. It kind of predicts it is more likely than not.

Mr. MCFARLAND. I agree.

Mr. CONNOLLY. Okay.

Mr. MCFARLAND. A high risk, for sure.

Mr. CONNOLLY. You also indicated it will cost too much. Do you want to expand on that a little bit?

Mr. MCFARLAND. Well, the $93 million that's set aside at this point won't come close. The migration itself is going to be an extremely costly measure.

Mr. CONNOLLY. Right. One would note that the CIA used an outside vendor, and I think they spent $600 million, but their system seems to be working. But it cost $600 million, I think, over 10 years, if I am not correct. Ring a bell? Sound right?

Mr. MCFARLAND. I'm not familiar with that, sir.

Mr. CONNOLLY. Worth looking at, because they partnered with the private sector rather than try to find all the answers inside.

Ms. Archuleta, what is your response to that IG flash audit alert?

Ms. ARCHULETA. The IG brought up some process issues that were very important, I think some that we don't agree with, but there are other areas that we do agree with.

I think the important thing is to underscore the relationship that we have with our IG. And we will continue to value his opinion and to bring forth his ideas into the considerations that we make.

I do believe that we have to move carefully but we have to work swiftly. As you said, these aggressors are spending a lot of money—a lot of money to get into our systems.

We need his assistance. We will seek his guidance. We will listen carefully to his recommendations and certainly consider those as we move forward.

Mr. CONNOLLY. Just a final note, Mr. Chairman. I introduced the Federal Agency Data Breach Notification Act of 2014. Unfortunately, although we blended that on a bipartisan basis into the Safe and Secure Federal Websites Act, the Senate did not act.

Had we acted, we would have had protocols in place for dealing with this kind of breach, at least after the fact, so that, you know, we could reassure the victims, who are Federal employees and Federal retirees. And I would hope that this committee once again will help prod the system, as it did last year, only this time getting the Senate to act, because that is really important.

Thank you, Mr. Chairman. My time is up.

And, again, thank you to my dear friend from Pennsylvania.

Chairman CHAFFETZ. [Presiding.] I thank the gentleman.

I now recognize the gentleman from Texas, the chairman of the Subcommittee on IT, Mr. Hurd, for 5 minutes.

Mr. HURD. Thank you, Mr. Chairman.

My mom always told me that you can always find the good in any situation, so let me try to start off with that.

DHS caught them, caught the problem, right? I think that is a good thing. When they were engaged, we found it. Wish it was a little bit sooner, but we caught the problem, so that is good.

I also got a letter from the Chief Information Officer of OPM. I am going to read a little bit.

"Dear Mr. Hurd, I am writing to inform you that the U.S. Office of Personnel Management recently became aware of a cybersecurity incident affecting its systems and data, and you may have been exposed. You are receiving this notification because we have determined that the data compromised in this incident may have included your personal information, such as your name, Social Security number, date and place of birth, and current or former address."

I know Ranking Member Cummings and Mr. Mica were talking about how could an adversary use this information. I spent 9 years as an undercover officer in the CIA. I think I have a little bit of idea and perspective on this.

If it was the Chinese, any Federal official traveling to China, former official, someone there is a subject of being targeted for elicitation of information about what is going on in the Federal Government.

If it was the Russians, all this information is going to be sold and then used against them to drain people's bank accounts, use this to create new access codes to get into private information.

If it was narcotraficantes in Mexico, which have the capability of doing cyber attacks, it is the home addresses of men and women in Border Patrol, people that are keeping us safe, right?

So the threat is huge. The impact is fantastic.

And one thing my dad always said was, "It never hurts to say you're sorry." And further in this letter, it says, "However, nothing in this letter should be construed as OPM or the U.S. Government accepting liability for any of the matters covered by this letter or for any other purpose." Later, it says, "We regret this incident." "I'm sorry" actually goes a long way.

Now, I agree with what my colleague from Virginia had said about this long, committed attack by advanced, persistent threats. And my issue is actually not with how we responded to the threat, because I think the immediate technical steps that were taken were good things, right? And I believe all the folks involved in the mitigation of the immediate threat were doing some things that I think can be used in other places.

But what I have a problem with is everything before this. If you were in the private sector, the head of a publicly traded company, and Ernst & Young was doing your yearly audit, and you had at least 5 years of audit information saying that your digital infrastructure had some high risk to it and needed to be immediately fixed, the board of directors would be held accountable for criminal activity, multiple years.

I did this for a living. I would penetrate the networks of companies and identify the problems that they had. And a lot of times, if there was a high-risk issue, we would call the customer immediately and say, "This has to be fixed right now," and the company and the customer would do that immediately. And so then, you know, we would issue our report, saying, "Here was the high-risk report, but it was fixed." Because a company like Ernst & Young doing an audit would probably not even put this information into an audit report to go to the board, because it is, "Guys, y'all gotta fix it." So my problem is that these high-risk issues that were identified by the IG haven't been addressed.

KeyPoint—and I guess my first question is to Ms. Ann Barron-DiCamillo.

Has US–CERT reviewed KeyPoint's network?

Ms. BARRON-DICAMILLO. Yes, sir. We were on site last summer at KeyPoint's network in Loveland, Colorado. And we were there with our interagency protesters and did an assessment of the network.

We actually went there in an abundance of caution based off of the event that happened both at USIS and OPM. It was decided by leadership that we needed to take a look at contractors that were performing background clearance investigations.

So there wasn't an indication that led for us—or led our teams to go on site, as the case with OPM. This was done out of an abundance of caution because of the target that we saw associated with background clearance information.

Mr. HURD. Thank——

Ms. BARRON-DICAMILLO. So our team did an assessment, a network integrity assessment. Some results came back that caused some concern, so we sent an incident response team on site and reviewed their network. We were there for a couple of weeks last summer.

Mr. HURD. When we hire contractors, are they subject to the same standards of network hygiene that U.S. Government networks are?

Ms. BARRON-DICAMILLO. Are contractors subject to the same? It would be part of the contract language associated with FISMA requirements. There's FISMA requirements that are—for any kind of network that houses government data, there are certain requirements, per the FISMA law of 2002.

Mr. HURD. And, Mr. Chairman, my last question.

In his opening remarks, Ranking Member Cummings read some of Director Archuleta's comments to the Senate committee. "The adversary leveraged a compromised KeyPoint user credential to gain access to OPM's network."

And then the written information that KeyPoint submitted said, "We have seen no evidence of a connection between the incursion at KeyPoint and the OPM breach that is the subject of this hearing."

Mr. Hess, feedback?

Mr. HESS. Congressman Hurd, it is true that the KeyPoint incursion, we've seen no evidence of a connection with the OPM incursion——

Mr. HURD. So are you saying that Ms. Archuleta is lying?

Mr. HESS. No, I'm saying she is correct. From knowledge that I have been given, there was an individual who had an OPM account that happened to be a KeyPoint employee and that the credentials of that individual were compromised to gain access to OPM.

Mr. HURD. Thank you.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We will now recognize the gentlewoman from the Virgin Islands, Ms. Plaskett, for 5 minutes.

Ms. PLASKETT. Thank you. Thank you very much.

Good afternoon, everyone.

I think that it is very interesting—I was listening to Ranking Member Cummings talking about the vulnerability of government contractors and the questions of my colleague Mr. Hurd regarding whether or not companies that have government contracts must keep the same level of security and care that the OPM or other agencies would have to, in terms of preparing for cyber attacks.

Mr. Giannetta, I have a letter that was sent from USIS to Ranking Member Cummings on December 5 of 2014, and the letter says that the Federal agencies have the failure of the company. And I wanted to ask you some assertions that you made in that letter.

In the letter, it says—their counsel wrote that the critical cyber attack defense information only flowed in one direction, from USIS to the government. Is that correct?

Mr. GIANNETTA. In the discussion we had earlier about the shared responsibility to notify from a contractor to the government and the government to the contractor, that is correct.

Ms. PLASKETT. You are qualifying it now. So you are saying that in terms of——

Mr. GIANNETTA. I'm not qualifying it. I'm suggesting that we were required and obligated by our contract to notify OPM that we had an intrusion, which we did immediately. And in the discussion

that was held earlier, OPM recognized that they did not notify USIS or, I believe, KeyPoint of their intrusion of March of 2014.

Ms. PLASKETT. So, in terms of the cyber defense information, was it one-way or did it go both ways?

Mr. GIANNETTA. In my humble estimation, it was one-way.

Ms. PLASKETT. So it was from yours to the others.

What would have, in your estimation, been the requirement of OPM or others towards you?

Mr. GIANNETTA. Well, I'm not a lawyer or a contract expert. I don't have the contract in front of me. But my understanding is that there's a requirement to notify, to say, we've got an issue, here's what the issue is, so that there's a free flow and sharing of information.

Ms. PLASKETT. So, if you have an issue, you are supposed to let them know, correct?

Mr. GIANNETTA. That's correct.

Ms. PLASKETT. And that is what you felt you did.

Mr. GIANNETTA. Absolutely.

Ms. PLASKETT. And then U–CERT, did U–CERT then—what did they do about that information that you gave them?

Mr. GIANNETTA. The CERT team?

Ms. PLASKETT. Yes.

Mr. GIANNETTA. We invited the CERT team to our facilities in Grove City, PA, formally via a letter. And the CERT team arrived shortly after receiving that letter and enumerated our network and understood through discussions with our technicians as well as the third party that we hired what had transpired from the 5th of June through the time they arrived.

Ms. PLASKETT. So why does your letter also state that U–CERT has not provided USIS with any sort of briefing regarding information it may have uncovered during the course of its limited review?

Mr. GIANNETTA. Let me just be clear that I didn't write the letter you're referring to.

Ms. PLASKETT. You are here testifying for your company. Your attorney—I am an attorney. I would never write a letter, as an attorney, for a company without the entire company agreeing to that.

Mr. GIANNETTA. I'm just suggesting that I didn't write the letter.

Ms. PLASKETT. But you are here to testify for the veracity of the letter. Was the letter correct or no?

Mr. GIANNETTA. We did not receive a briefing from CERT as to the findings that they had vis—vis the intrusion. We did receive——

Ms. PLASKETT. Okay. Then let's ask CERT, since they are here.

Mr. GIANNETTA. If I could finish, we did receive some recommendations relative to what we might do to——

Ms. PLASKETT. That is not a review?

Mr. GIANNETTA. Our invitation to CERT requested their assistance in identifying threats to our network, and we did not receive that.

Ms. PLASKETT. Okay. Well, let's ask Ms. Barron-DiCamillo.

Can you speak to that?

Ms. BARRON-DICAMILLO. Yes.

So our team was on site. It was an interagency response team including our law enforcement partners. We worked—just part of

the incident response team, what we do is we're working with the system administrators daily. We're informing them every day at the end of the day of——

Ms. PLASKETT. How many days did you inform them on a daily basis?

Ms. BARRON-DICAMILLO. We were there for about 2 weeks. I'd have to go back and get the specific timeframe.

Ms. PLASKETT. So that's at least 10 reports that you've given them.

Ms. BARRON-DICAMILLO. We worked through the weekend, ma'am.

Ms. PLASKETT. Through the weekend?

Ms. BARRON-DICAMILLO. Yes.

Ms. PLASKETT. So that's 14 reports that they were given asserting what the issues were.

Ms. BARRON-DICAMILLO. The daily findings. And they can change, so that's why we——

Ms. PLASKETT. And did you find something, and did you give them ideas about what needed to be done?

Ms. BARRON-DICAMILLO. Yes. We were able to discover that there was malicious malware present on the network, that there was compromised credentials, specifically——

Ms. PLASKETT. And how did that happen? How did those compromised credentials—what were the two areas that you found within their own system that should have been taken care of previously?

Ms. BARRON-DICAMILLO. We found a lack of some security mechanisms that would have helped to prevent this kind of intrusion, but, because of the lack of logging, we weren't able to find the initial point of entry. We were able to find——

Ms. PLASKETT. Can you talk about that, the lack of logging? What is that?

Ms. BARRON-DICAMILLO. There's a number of types of logs that we look at forensically that can help us piece together a picture of what's happened within your network.

Ms. PLASKETT. And why weren't those there?

Ms. BARRON-DICAMILLO. I suppose a number of reasons. It's a risk decision, a risk-based decision. It can cost a lot of money, depending on the volume.

Ms. PLASKETT. It is a risk and a cost decision made by the company itself.

Ms. BARRON-DICAMILLO. It can be, because it can require quite a bit of storage associated with some of the kinds of logs.

Ms. PLASKETT. So the government contractor that we hired to do government work for us decided that a risk and a cost decision on their part did not require them—they didn't put in the logins that were necessary to protect the system.

Ms. BARRON-DICAMILLO. I can't answer that specifically. I can just give you some of the reasons I've seen, that people are not continuing to have the historical logs because of the volume of data. You know, there's millions of net flow records that happen a day, and that does require quite a bit of storage. And——

Ms. PLASKETT. So the letter that was sent by USIS to Ranking Member Cummings, would you agree with the assertions that were made there?

Ms. BARRON-DICAMILLO. No, I would not. We did provide them daily reports as well as a final findings report. We went over that with the team. And then we also provided a mitigation report. And I have documented evidence of all of that.

Chairman CHAFFETZ. I thank the gentlewoman.

Did you want to respond to that?

Mr. GIANNETTA. If I may.

Chairman CHAFFETZ. Sure.

Mr. GIANNETTA. It's my understanding from our forensic investigator, Stroz Friedberg, that what was found by the CERT team vis—vis Ms. Barron-DiCamillo's comments was not information that they hadn't already discovered. In other words——

Ms. PLASKETT. So the logins that were needed for them to be able to go and do a deeper forensic was something that they already knew?

Mr. GIANNETTA. That——

Ms. BARRON-DICAMILLO. I think what he's saying——

Ms. PLASKETT. Yes or no, did they already know?

Ms. BARRON-DICAMILLO. —is we confirmed the forensic evidence of the third-party partner.

Mr. GIANNETTA. Thank you.

Ms. BARRON-DICAMILLO. Right. So I believe what he's saying is, it sounds a bit of a—you know, it was a confirmation. And we were able also to confirm the compromised credentials associated with the third-party forensic firm that they had in there. And then we were able to discover additional findings throughout the assessment that we did.

Chairman CHAFFETZ. I thank the gentlewoman.

We will have to further explore that, but, for now, we will recognize the gentleman from Alabama, Mr. Palmer, for 5 minutes.

Mr. PALMER. Thank you, Mr. Chairman.

Ms. Archuleta, last week, I brought up a letter from two of my legislative staffers received warning them that their personally identifiable information may have been compromised in the cybersecurity hack.

I bring this up again because, earlier, you disputed the number of people that are affected by this when Ms. Seymour admitted, after I questioned her about the letter that she signed, that this goes beyond the people who filled out the Form 86.

And I just want to know, considering the fact that a vast amount of personally identifiable information stored by OPM was vulnerable due to the login credentials, was it likely exposed by foreign contractors, outsourced by OPM and OPM's failure to communicate with and abide by the IG's recommendations?

Ms. ARCHULETA. I'm sorry, sir. Could you repeat that question?

Mr. PALMER. I am just asking you, do you—let me rephrase it. Do you standby your assertion that this is limited to a smaller group than is being indicated in the media and might be indicated by the fact that this extends beyond the people who filled out Standard Form 86?

Ms. ARCHULETA. Thank you for clarifying the question, sir.

I think it's really important not to conflate to the two incidents. The first incident was the employee personnel records, which is the 4.2 million.

Mr. PALMER. That is not—I am just asking——

Ms. ARCHULETA. And the second——

Mr. PALMER. —is it more than 4.2 million?

Ms. ARCHULETA. And the second incident, we haven't determined the number yet, of the scope of that incident and the number of employees that would have been affected by that and others.

Mr. PALMER. Okay. So the answer is yes, that it is more.

I think it is very evident that this attack on the Federal employees' personally identifiable information not only puts those workers at risk but also puts secondary groups at risk. For instance, if they have their personal email addresses, as it is pretty evident from, as I pointed out last week, that some of the breaches occurred through personal email addresses, that all of these employees and their secondary relationships, is it possible that certain information was exposed there as well?

Ms. ARCHULETA. Yes, the team that is working on the analysis of the scope is—it's exactly why we're taking our time to make sure that it's accurate. And the SF–86s we've talked about earlier. The data in there is—includes not only the employee but may include other information and PII for other individuals. That's why we're being very, very careful about that and looking at the data, because it could be that there was no PII for some individuals.

Mr. PALMER. But, ma'am, beyond the SF–86s, I am talking about where the breach apparently occurred, as well, through personal email addresses, particularly at the Immigration and Customs Enforcement Agency, that was reported in The Wall Street Journal.

I brought this up to you last week. I will be happy to provide this information to you——

Ms. ARCHULETA. Yes.

Mr. PALMER. —if you need to see it. But where they got in on personal email addresses, that would expose everybody in their email chain.

Ms. ARCHULETA. Ah. I'm sorry. Yeah.

Mr. PALMER. And I think we have——

Ms. ARCHULETA. I understand your question.

Mr. PALMER. Let me go on to something else.

You received a letter last week from Senator Mark Warner with some specific questions about a contract that you awarded to CSID. Have you responded to Senator Warner's letter yet?

Ms. ARCHULETA. I'd have to check with my staff, sir. I know——

Mr. PALMER. Have you——

Ms. ARCHULETA. —that we were attempting to respond as quickly as possible, yes.

Mr. PALMER. Have you personally read his letter?

Ms. ARCHULETA. I have read his letter, but I have not—I don't know that our response has made it through our system yet.

Mr. PALMER. All right.

He raises a question here about how quickly this contract was awarded to CSID. You didn't go through the normal process, and it was awarded in 36 hours, I think, is what Senator Warner says.

Was it intentionally steered to CSID?

Ms. ARCHULETA. No, sir.

Mr. PALMER. Who made the decision?

Ms. ARCHULETA. I would ask Donna to talk about the process that we used. It was a fair and competitive process.

Mr. PALMER. A fair and competitive process.

Ms. SEYMOUR. Our contracting officer made the selection on the contract, sir.

Mr. PALMER. Okay. Did you evaluate the management of CSID?

Ms. SEYMOUR. I did evaluate both the technical and the cost proposals for——

Mr. PALMER. Did you evaluate the people who run the company?

Ms. SEYMOUR. I had resumes for the people—or for the key personnel that they provided in the proposal.

Mr. PALMER. Are you familiar with their board of directors?

Ms. SEYMOUR. No, sir, I'm not.

Mr. PALMER. Okay. Do you know Owen Li, one of their directors?

Ms. SEYMOUR. No, sir, I don't.

Mr. PALMER. Okay.

Mr. Chairman, my time has expired. I yield the balance.

Chairman CHAFFETZ. From start to finish, how long was it from when you got the proposal that you awarded the contract?

Ms. SEYMOUR. I would have to go back and look at exactly when we released the RFQ. But I believe it—and I don't want to misspeak. So let me go back and find out when exactly we released the RFQ and exactly when we awarded the contract. I don't have that data with me.

Chairman CHAFFETZ. But it was less than 48 hours, right?

Ms. SEYMOUR. I think it was about in that timeframe, sir.

Chairman CHAFFETZ. And the award is how much money?

Ms. SEYMOUR. The contract is about $21 million for the services that we're providing for credit monitoring, notification, and the identity theft insurance.

Mr. CUMMINGS. Will the gentleman yield?

Chairman CHAFFETZ. Sure.

Mr. CUMMINGS. Why was it made so fast?

Ms. SEYMOUR. We wanted to——

Mr. CUMMINGS. And was there other companies that could do just as good a job? I am just trying to figure out how we got that company.

Ms. SEYMOUR. We received a number of proposals, and we evaluated them based on the government's needs, several requirements that we had put in the RFQ that the companies responded to. And we evaluated all of those proposals that we received against that criteria, and Winvale provided the best value to the government based on those requirements.

Chairman CHAFFETZ. Will you also copy—when you give Senator Warner the answer to his questions, will you send us copies of that, as well?

Ms. ARCHULETA. Yes.

Ms. SEYMOUR. Yes, sir.

Chairman CHAFFETZ. Okay. Thank you. I think he raises a number of important questions, as does Mr. Palmer here, and we will continue to pursue that.

We now will recognize the gentleman from Pennsylvania, who has been waiting patiently, Mr. Cartwright, for 5 minutes.

Mr. CARTWRIGHT. Thank you, Mr. Chairman.

Mr. Chairman, I find myself utterly dissatisfied with the explanations we have heard today.

And I want to train my attention on you, Mr. Hess. You have made some fine distinctions about what that employee of your company was doing, the one that got hacked and who was working on OPM's systems at the time. And, because of that hack, that employee became a victim and lost personal information. And that led to the successful hacking of OPM's systems.

Have I broadly described that correctly, sir?

Mr. HESS. We actually do not know how the employee's credentials were compromised.

Mr. CARTWRIGHT. All right. But it was a KeyPoint employee; am I correct in that?

Mr. HESS. That is correct.

Mr. CARTWRIGHT. And you are the CEO of KeyPoint, right?

Mr. HESS. That is correct.

Mr. CARTWRIGHT. All right. And you are denying accountability for that hack, for the OPM hack. And what you said was the employee was working on OPM's systems at the time, not KeyPoint's. That is what your testimony was, correct?

Mr. HESS. That is correct.

Mr. CARTWRIGHT. Well, so we have an individual's OPM credentials that were taken. That individual happened to be a KeyPoint employee. Did that KeyPoint employee have OPM credentials as part of his or her scope of employment with KeyPoint?

Mr. HESS. Correct.

Mr. CARTWRIGHT. Okay. It wasn't a coincidence that this KeyPoint employee had OPM credentials. It was part and parcel of his or her scope of employment with your company, wasn't it?

Mr. HESS. That is correct.

Mr. CARTWRIGHT. All right.

And it was KeyPoint paying this person as the person was working on OPM's systems at the time; am I correct in that?

Mr. HESS. That is correct.

Mr. CARTWRIGHT. And you understand, under traditional concepts of the law, KeyPoint is responsible for the acts of its employees acting within the scope and course of their employment with your company. You understand that, don't you?

Mr. HESS. I'm not familiar with that construct.

Mr. CARTWRIGHT. All right.

Mr. Hess, you are here today because a cyber espionage operation succeeded in breaching very personal information that your company was entrusted with.

On January 6, 2015, my ranking member, Mr. Cummings, sent you a letter requesting information about the data breach. His letter requested a number of documents. Did you get the letter?

Mr. HESS. Immediately upon receiving the letter, KeyPoint counsel reached out to the ranking member's staff to arrange for a briefing. And we tried to have a date and time set up, and we are still waiting for confirmation on that.

Mr. CARTWRIGHT. You got the letter, right?

Mr. HESS. Yes, sir.

Mr. CARTWRIGHT. And more than 5 months later you haven't responded with documents; am I correct in that?

Mr. HESS. We reached out immediately to the ranking member's staff to brief the staff, and we have not received a response on a time and day to do so.

Mr. CARTWRIGHT. Well, let's go through the document request that Mr. Cummings made.

He requested a log of all successful cyber intrusions into your company's networks in the last 4 years. That is a reasonable request, isn't it, Mr. Hess?

Mr. HESS. I don't find it unreasonable.

Mr. CARTWRIGHT. Will you provide this to the committee?

Mr. HESS. I will take that back to my team and let you know.

Mr. CARTWRIGHT. You are the boss there, aren't you?

Mr. HESS. I am the CEO.

Mr. CARTWRIGHT. All right. But you are going to get permission from your team, who work for you; is that it?

Mr. HESS. I'm going to take it back and discuss it with my team.

Mr. CARTWRIGHT. Let's go to the next request: copies of all forensic analyses and reports concerning the data breach, including findings about vulnerabilities to malware.

When will you provide these documents to the committee?

Mr. HESS. I'll take that request back to my team and let you know.

Mr. CARTWRIGHT. Ranking Member Cummings requested a list of all Federal customers affected by the data breach. Will you provide those to the committee?

Mr. HESS. I will take that back to my team and let you know.

Mr. CARTWRIGHT. Mr. Hess, your company exists because of the largesse of the United States Federal Government. We expect you to respond to requests from this committee.

Mr. Cummings does not write letters because he just enjoys writing letters. He is concerned about the security and the safety not only of Federal employees but of the United States public.

This is really important. Will you please treat it as such?

Mr. HESS. I do, Congressman Cartwright. Just—we responded immediately to Congressman Cummings' request by calling their staff, having our counsel. And I would also inform——

Mr. CARTWRIGHT. By responding and calling but not providing the documents. We want the documents, Mr. Hess.

I yield back.

Mr. CUMMINGS. Will the gentleman yield?

I just want to clear this up, because you just said some things that—you talked about my staff.

Mr. HESS. Yes, sir.

Mr. CUMMINGS. And it is my understanding that they did get back to us, but for months—for months, some back-and-forth because you all did not want to agree to the scope of the meeting.

And then, just recently, because of this hearing, you finally said, scrap the limitations on the meeting, the scope, and we'll meet.

And so I don't want you to, you know—I don't know whether you have the information or what, but I want you to be accurate.

Mr. HESS. That's not the information that I have, sir.

Mr. CUMMINGS. Well, then your information is inaccurate.

Mr. HESS. I will research that.

Chairman CHAFFETZ. Mr. Hess, is it reasonable by the end of this week to provide us the documentation on the communication and the lack of the meeting over the last several months? Is that fair? By the end of the week?

Mr. HESS. I will take that back to my team and get back to you.

Chairman CHAFFETZ. You are the CEO. You can make these decisions. Are you or are you not going to do that?

Mr. HESS. I'm going to take it back to my team and discuss it.

Chairman CHAFFETZ. No. That is not good enough. Give me a date that you think is reasonable to give us the correspondence dealing with setting up a meeting. It can't be that difficult.

Mr. HESS. Chairman Chaffetz, I was asked last week, on Wednesday, to brief both your staff——

Chairman CHAFFETZ. But you were asked months ago to brief the minority staff, and that didn't happen. I just want to see the documentation; is that fair?

Mr. HESS. I will take that request back to my team.

Chairman CHAFFETZ. No. I want an answer from you. I want to know when you will provide that information to this committee.

Mr. HESS. I will take that request back——

Chairman CHAFFETZ. No. I want a—you give me the date. When is it reasonable? You are the CEO.

Mr. HESS. I understand, sir. I will take that request back to my team.

Chairman CHAFFETZ. No. I need an answer from you. All right, we will sit here all day if you want. You want me to issue a subpoena? Is that what you want me to do? Because I will sign it. I will sign it today.

Give me a date that is reasonable.

Mr. HESS. I need to take that information back to my staff.

Chairman CHAFFETZ. Sir, seriously, when are you going to provide that information?

Mr. HESS. I'm trying to be helpful, Chairman. I did do a briefing last week, and we did reach out to Congressman Cummings' staff immediately upon receipt of the letter. And we did not receive, by the information that I have——

Chairman CHAFFETZ. Am I asking for anything unreasonable, to provide the correspondence and the interaction? I mean, they are going to have their half. I just want to see your half. I am trying to give you an equal opportunity here.

Mr. HESS. I understand that, sir.

Chairman CHAFFETZ. When is it a reasonable date?

Mr. HESS. Let me get back to you with that information.

Chairman CHAFFETZ. No. I want you to decide before the end of this hearing. We are going to go to the next set of questioning. You can counsel with all the people that are sitting behind you, but it is a reasonable question. What Mr. Cartwright said is not unreasonable. And so, if you think it is, tell me. But I just want to see the correspondence.

Counsel all you want while we ask the next set of questions, but I suggest you keep an ear to Mr. Grothman, who we are going to recognize for 5 minutes.

Mr. GROTHMAN. Thank you.

Two comments before I ask questions. First of all—and this is kind of a followup on what I think Congressman Hurd was trying to get at—it surprises me you folks are not more contrite over what happened. It seems like you don't understand the enormity of the disaster that has happened here.

Secondly, I think sadly this is all too often common for government, and it is something that I think everybody in this institution should remember as we pass bills having the government have these huge data banks of educational information or medical information or what have you. Because if the people in charge of these banks of information don't display more sense of urgency than you folks, I think, you know, the possibility of this happening at other agencies is something we should be considering.

But now I have some questions for Ms. Seymour.

You are going to be in charge of a whole overhaul of this whole IT thing, correct?

Ms. SEYMOUR. Yes, sir.

Mr. GROTHMAN. Do you feel you have got the skill set to oversee something of this magnitude?

Ms. SEYMOUR. I don't ever believe that I have the skill set to do something this large. And that's why I employ people who have a broader skill set or a different skill set than me in various areas. I don't have all the technical skills that I would need to do something like this. It takes a team.

Mr. GROTHMAN. Okay. In your past positions, have you overseen—what were the largest projects that you have overseen, IT projects in your prior work experience?

Ms. SEYMOUR. I have overseen some very large projects, sir, both in my past employment with Department of Defense as well as the Department of Transportation. Systems that were certainly enterprisewide and served large populations of people like OPM.

Mr. GROTHMAN. Sizewise similar to——

Ms. SEYMOUR. Yes, sir, sizewise similar.

Mr. GROTHMAN. And how quickly were they able to complete these projects?

Ms. SEYMOUR. Some of them took—some of them were much faster than others. You know, it depended on when I came into them. Some of them were delivered within a year, and some of them took years, multiple years to deliver. I think sometimes the way that we're changing the way that we deliver IT solutions now, we're trying to be much more agile. And so we're trying to find what we call a minimal viable product. We are trying to find segments of capability that we can deliver in shorter term. So we are trying to deliver, you know, capability within 6 months, 6-month segments, and then build on that to get to a whole system.

Mr. GROTHMAN. And how quickly do you think you will be able to complete this current project? Do you have a goal or an expectation?

Ms. SEYMOUR. When we started the project, sir, we kind of divided it into two pieces so that we could understand it. The first we called our tactical phase, which was shoring up the network that we have today. And we have put a great number of security

tools into our current network. And that's what allowed us to find this adversarial activity this year.

The second piece of this was building the shell. And we estimated that it would take us approximately a year to be able to deliver that. That project is on schedule, and it is on budget. And we will be delivering the shell environment this fall.

The next phase is migration. And we have recognized from the very beginning that we did not have a full enough scope, certainly not from my tenure on board back to June of 2014, that I have enough scope or understanding of exactly the OPM—the full OPM environment to be able to assess what it was going to take to do that migration. And so that's why we only contracted for the first two pieces. And we said as we worked through this project, to understand it, we will be able to better estimate and understand what needs to move into that shell. But we knew from the beginning that there were some systems that were very old, that are about 30 years old, that we were going to have to migrate into that shell. So we focused on those first.

Mr. GROTHMAN. Okay. One other question. Last time you were before this committee, you referred to the fact that you deal closely with the IG. And last time we had a major IG project you apparently did not notify him of the project. Do you have a reason for that or an explanation for that?

Ms. SEYMOUR. I am not aware of a requirement, and I certainly could be corrected, but I am not aware of a requirement to notify the IG of every project that we take on. Certainly we included in our budget request for 2016, we talked through this project and documented it in that arena. We also discussed on a couple of occasions with the IG this project because they have an interconnection with our network. And some of their systems, we actually host some of their systems. And so they have to come along with us in this project if we are going to continue to provide those services.

Mr. GROTHMAN. Okay. But an undertaking of this size, you know, maybe it's not something you normally tell the IG about, but you would not have felt the necessity to notify them what's going on here?

Ms. SEYMOUR. Sir, it's just based on my experience that if I am—no, sir, I would not normally advise the IG of a project that we are doing. That doesn't mean I am holding the information from them. But I also do know that we discussed with the IG on a number of occasions the fact that we were taking on this project and that they needed to modernize their systems and upgrade their systems to be able to meet the security requirements for this project.

Mr. GROTHMAN. Okay. Thank you.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognized the gentlewoman from New Mexico, Ms. Lujan Grisham, for 5 minutes.

Ms. LUJAN GRISHAM. Thank you, Mr. Chairman.

I just got back down to this hearing after a meeting in my office with the leadership of one of the five national labs, Sandia Laboratories, which is in my district, Albuquerque, New Mexico. And, of course, the theme of many of those meetings are the constant threats. Every second of every minute of every day, they are clear that someone, something is entertaining a cybersecurity attack.

And it's a constant threat. And they're clear that that's the environment that they work in. They are also clear that they need our support and recognition to be proactive and to do something about these problems both internally and externally. And I appreciate their constant surveillance and their awareness of this critical problem.

I too—before I ask my question—am extremely disappointed in the reaction from this panel at this hearing, that we know that these are issues that we have to deal with, that we are in fact accountable, and in fact you are liable. And what I hear is that none of those really are occurring, that if you don't provide us the answers at this hearing and the answers that we are requesting in the documents, you cannot help us assure that we are protecting or adequately identifying the scope, which means that then you become part of the problem again. And I find it incredibly offensive that that's what is occurring in this hearing. What we all ought to be doing is assuring that we are protecting not only the thousands of Federal employees in my district, and the hundreds of thousands of employees around the country, and the millions of employees who are affected, we are all scrambling to figure out who is the most accountable and who is the most responsible and who is the most liable. And I am expecting much better cooperation.

There is a lot of work to do in accountability, identifying the scope, doing something about the legacy systems, making sure we are prepared for the next potential breach. And as we do that, I do want to focus on how we are treating these employees. And so, Director Archuleta, I hold in my hand one of the letters that many of my employees and my constituents are getting. And I am concerned about some of the aspects of the letter, and want you to talk me through about some of the concepts identified in the letter and how you came to these conclusions and what we might do to broaden those. For example, in the letter, you say that, your information—to an employee—could have been compromised, that potentially affected—I don't know when you are going to find out about that—will receive a subscription to CSID, protection and identity theft, for 18 months. Now, what happens if you have an issue after the 18 months? Is that individual going to be covered?

Ms. ARCHULETA. The individual on the identity theft, yes.

Ms. LUJAN GRISHAM. So even though the letter says you have got an 18-month, when are we going to know in writing? Because these are lifetime issues. Unfortunately, they don't go away. Once that's been compromised, that's the problem, you're compromised. I don't think that these consequences are just 18 months. And I was interested in how you came with that framework. It seems to me people should know that they're going to be protected by you and supported, irrespective of the timeframe.

Ms. ARCHULETA. I understand your concerns. And I understand the responsibility that we have to our employees about their PII. I take that responsibility very, very seriously. I want to say that there are—in the letter, the first sentence that you wrote, the difference between exposure and exfiltration. It could be that their data was exposed and not exfiltrated. But we feel strongly that we need to offer the same protections to those employees who their data might only have been exposed.

Ms. LUJAN GRISHAM. I got it. But I want to know that you are going to be responsible and supportive of these employees.

Ms. ARCHULETA. Absolutely.

Ms. LUJAN GRISHAM. Not just in the short term, but the long haul. So they can expect maybe another letter, something that says, "We are here," because the other thing I would like you to consider—and I appreciate that response—is that if you look at the letter, again, and I read it carefully, we are pushing folks, I get also, I agree, to the right kinds of experience, I hope, contractors to provide that support and identity restoration. I would like more clarity about what that will involve.

Ms. ARCHULETA. Sure.

Ms. LUJAN GRISHAM. But in addition, you have got to call all these outside numbers. You have to call all these credit agencies. You have to enroll yourself. I would really strongly encourage you that there ought to be a phone number that I can call to OPM.

Ms. ARCHULETA. By law, they have to enroll in the credit monitoring.

Ms. LUJAN GRISHAM. I understand that part. But in terms of managing and supporting employees, I expect that the organization that's the source of the breach would be available to me and not just outside numbers. And I don't know if you have done any mystery shopping of the toll-free numbers or calling these credit folks, but there is an interesting long waiting period. I would really strongly suggest that we step up H.R. and that there is a quick and immediate response in your own department.

Ms. ARCHULETA. Thank you. I appreciate your comments.

And I agree with you totally that we need to hold our contractor responsible for their response. We are also instituting new ways that they can respond to the employees. I think I mentioned before you got here is that we are using the SSA model where we in fact are being able to call them back, that no one has to wait on line.

Chairman CHAFFETZ. I thank the gentlewoman.

We will new recognize the gentlewoman from Virginia, Mrs. Comstock, for 5 minutes.

Mrs. COMSTOCK. Thank you, Mr. Chairman.

Thank you for letting me sit in on this hearing. And I think, as I have already talked with OPM, we do plan on doing some hearings in the Science and Technology Subcommittee, which I chair also. Like some of my colleagues have already mentioned, and they have had that experience, I have received those same letters, as have, more importantly, tens of thousands of my constituents here in northern Virginia, like Mr. Connolly.

I also had the unfortunate experience of also getting a letter from the IRS saying my tax information had been compromised. But that's probably another hearing, Mr. Chairman.

But what I am concerned about is I am not hearing leadership here. I know when I visit the Visa data center in my district, and I see all the things they have in place and the leadership they are exerting there and the leadership that comes from the top there, I see a very strong culture of leadership in their cybersecurity and how they are attacking it.

So my question, Ms. Archuleta, now when you came here 18 months ago, you understood that we had a very real threat from

China and other bad actors, that this was constant, like the Congresswoman was just talking. It is constant. It is something every day, and it is something you are always going to face. Do you understand that?

Ms. ARCHULETA. Yes, I do.

Mrs. COMSTOCK. Okay. So, in doing that, because I think really what we know here from what Mr. Connolly said, I think what we have all recognized is they are at war with us. And we aren't up to speed. And we aren't responding in kind in terms of the problem. Now, what I am hearing is the blaming the actor here, saying that, well, we know they are bad actors. And we know that; that's part of the job. So what I would like to know is in the 18 months, how many meetings have you had yourself personally where it's been exclusively about cybersecurity, and you have had those meetings, and who have they been with?

Ms. ARCHULETA. I have had those meetings with individuals throughout government. I have had those almost on a daily basis with my own staff and the CIO. I would say that since the 18 months that I arrived, I recognized the same problem that you did. And we have taken tremendous steps but, as you say, that there are these actors, and they are aggressive, and they are well funded, and they are persistent. And the first thing I did was to implement an IT strategic plan with a focus on IT security.

Mrs. COMSTOCK. I appreciate that because we have gone through those details. Have you visited a private sector, a data center and seeing what the private sector does?

Ms. ARCHULETA. I have had discussions with the——

Mrs. COMSTOCK. No, have you visited? Have you visited someplace?

Ms. ARCHULETA. I have visited other, yes, other companies. The issue of cybersecurity was not the one that we discussed. But as the plan that I outlined this morning is that we are holding a summit in the very near future to bring those private individuals who are facing the exact same threats that we are so that we can learn from them. We need to access experts.

Mrs. COMSTOCK. But in the past 18 months, you had not done that?

Ms. ARCHULETA. I have not met personally on cybersecurity issues.

Mrs. COMSTOCK. Okay. With the private sector.

Ms. ARCHULETA. With the private sector. But my colleagues from across government have, like Tony Scott and others, the Federal CIO. And I have been the benefit of those conversations and his experiences, as well as other people throughout government. We recognize that cybersecurity is an enterprise issue for all of us in government. And it's not just one person who has to take responsibility. All of us across government have to.

Ms. COMSTOCK. I appreciate that. But I think the point that has been made to me by people who are leaders in this field is the person at the very top has to take that role. And I would note that when Target, when they had this breach, when they had this problem, it wasn't just their CIO that lost their job, it was the CEO who lost their job. And that's how that was responded to in the private sector. So I want to continue with some of the points that

have been made by Mr. McFarland. Have you sat down with Mr. McFarland to discuss his recommendations? You personally.

Ms. ARCHULETA. I sit with Mr. McFarland. He has brought some of those to my attention. I also, with the flash audit, I have not had the opportunity because of the time period that it was released. But it's my full intention not only to talk with him about the flash audit but also to engage him as we move forward, as we always have.

Mrs. COMSTOCK. Okay. Now, when I sent you the letter that you had sent back, really one of the questions I had in there was how many people in my district have been impacted by this? I think it's a fairly simple question because you sent out the 4.2 million letters, right? And letters usually have a ZIP Code. So when you asked—you should be able to tell us how many people we have in our districts that have been impacted by this. I certainly have been hearing from many. And they have a lot of questions.

And I would like to also mention I would like to submit for the record questions from the Federation of Government Employees.

Mrs. COMSTOCK. And I have had a lot of incoming questions that have come that obviously we don't have time here. But just a simple question that did not get answered was, how many constituents do I have impacted by this?

Ms. ARCHULETA. I would be able to get you that information from our data, and we would be glad to share it with you.

Mrs. COMSTOCK. Okay.

Thank you, Mr. Chairman. I yield back.

Chairman CHAFFETZ. I thank the gentlewoman.

I will now recognize the gentleman from California, Mr. DeSaulnier, for 5 minutes.

Mr. DESAULNIER. Thank you, Mr. Chairman.

I apologize for having had to leave. Very troubling. I have what may be a character flaw for this committee. I tend to give the benefit of the doubt.

So, Ms. Archuleta, I would like to give you the benefit of the doubt, but the flash report really is quite concerning to me. So, Mr. McFarland, a quote from that says, "In our opinion, the project management approach for this major infrastructure overhaul is entirely inadequate and introduces a very high risk of project failure."

Having sat here and listened to multiple hours now in this hearing, would you say that your level of confidence in OPM is heightened, or do you stand by that comment?

Mr. MCFARLAND. I stand by that comment.

Mr. DESAULNIER. And you also asked for responses from OPM. It says you asked for it on June 2 of 2015, and you asked for comments by June 5, and then later extended that to June 10. By June 17, we had still not received comments or indication that comments would be forthcoming. Did you ever get comments back before the hearing?

Mr. MCFARLAND. I think we may have gotten comments back that day.

Mr. DESAULNIER. Okay. Well, I got something this morning, U.S. Office of Personnel Management, actions to strengthen cybersecurity and protect critical IT systems. It doesn't have a specific date,

June 2015. But, Ms. Archuleta, is this the response that you provided the IG, or is this for the committee? It is a 7-page report.

Ms. ARCHULETA. No, I am familiar with it, sir. The action plan that you received today is an action plan that I developed along with my staff in response to the very serious issues and threats that we are facing right now. It outlines what we have done and what we will be doing.

The response to the IG on the flash audit he has received. As I said before, Mr. McFarland and I have not had the opportunity because of the time period that where we have been engaged with other things. But it's our intent, as in the plan, to make sure that he is engaged with this alongside us, and that we value his opinion and the work of his staff.

Mr. DESAULNIER. So, Mr. McFarland, heretofore you haven't got that kind of impression—at least that's my impression from your testimony—I am sorry, you were distracted for a second.

Mr. MCFARLAND. Sorry.

Mr. DESAULNIER. That Ms. Archuleta said she valued your input and looked forward to working with you. But, heretofore, you haven't gotten that, from what I ascertained from your comments today and the written commentary.

Mr. MCFARLAND. Well, what is on paper is exactly what I——

Mr. DESAULNIER. Do you have any heightened confidence that what Ms. Archuleta just said about your relationship will improve? It doesn't seem there is any evidence to that.

Mr. MCFARLAND. Well, I think in general we have a good relationship. Just, I mean, truly, I think we have a good relationship. Regarding this matter, I think we are worlds apart.

Mr. DESAULNIER. That's fairly significant. As you said to Mr. Lynch, $93 million you said isn't even close to the amount needed in your opinion and that the ability to succeed—there is a high risk that these efforts will ultimately be unsuccessful. Given how horrible the consequences of what has already happened doesn't really give me a lot of confidence that going forward anything is going to improve. As a matter of fact, it sounds like it is going to get worse.

Mr. MCFARLAND. I think going forward at the right pace and concentration might be very successful. What I think is planned by OPM I think is dangerous.

Mr. DESAULNIER. Would you like to respond to that, Ms. Archuleta? And I can only imagine how difficult it is coming in here. But I must tell you, just sitting here and being willing to give you the benefit of the doubt, you appear to come across as petulant, defensive, and evasive.

Ms. ARCHULETA. I don't mean to do that at all. I take very, very seriously what has happened.

Mr. DESAULNIER. You said that over and over again. With all due respect, I believe you, but it doesn't appear to be the truth.

Ms. ARCHULETA. Well, I do—what I have tried to do today is to convey to the members how seriously I take this and that we are garnering all the resources, including the opinion of the IG. We disagree on some issues, but we do have other areas of agreement. We also have areas that would benefit from discussion between me and the IG. I think that's an important step. IGs work very closely with their administrations to make sure that we are doing the best job

we can. I take his information very seriously. I do not want to convey that I am angry or petulant about it. What I am is respectful for the position he holds and value the input that he gives.

But I do feel passionately about what has happened. I feel very passionate about the employees. I am a champion and have worked very hard throughout my entire career. And if I sound passionate about it, I have to say that I am.

Mr. DESAULNIER. So I just, personal observation, sometimes you can feel passionate about things but not be capable of doing what you desire to do. And I think we need to have a serious conversation. I know the chairman has these concerns about, to be perfectly honest, whether the current administration is competent enough to protect this information from people who would hack us.

Mr. CUMMINGS. The gentleman yield?

Mr. DESAULNIER. Yeah.

Mr. CUMMINGS. I think the gentlemen gets to the point that I was trying to get to a little bit earlier. And the question becomes we have got Mr. McFarland saying that—I think he used the word "dangerous." Is that what you said?

Mr. MCFARLAND. That's correct.

Mr. CUMMINGS. We are heading down a dangerous path.

Mr. MCFARLAND. I believe so.

Mr. CUMMINGS. And when you say "dangerous," you are saying we are headed for some very serious trouble. Is that a fair definition of "dangerous"?

Mr. MCFARLAND. Absolutely.

Mr. CUMMINGS. So, Ms. Archuleta, our problem is this: We sit here, and we have got an IG who we believe in and trust. The IG is saying that you need to take his advice, and what you are doing is not going to get us there, as a matter of fact, may harm us. Am I right, Mr. McFarland?

Mr. MCFARLAND. That's correct.

Mr. CUMMINGS. So you have put us in kind of a difficult situation. We have now been given notice as Members of Congress that we are headed down this path by somebody who we rely on. You disagree with him, but then you expect us to be supportive of you. No, no, no. Listen to me. That's a problem because now you put us in a kind of bad position.

So that means that if this happens again, problems get worse, then people say: Well, wait a minute, Chaffetz, Cummings, you all were sitting there. You heard what the IG said. I mean, why did you let this go on?

That's the position that we find ourselves in. And so I don't care whether you like each other or not. That doesn't matter to me. A lot of people get along. The question is it sounds like you are refusing—no, no, answer me now; I am going to give you a chance—to do what he has asked you to do because you disagree. But on the other hand, he is saying that we are going down a dangerous path. I mean, come on now. Do you have a comment?

Ms. ARCHULETA. Yes. I just wanted to be sure. The flash audit identified issues. A flash audit is meant to alert the administration about concerns. It merits an opportunity for the IG and his staff and my staff to sit down and find out where his concerns are. If he says it is a dangerous path, I want to know specifically why.

Mr. CUMMINGS. Mr. McFarland, haven't you told her that before? Is this new?

Mr. MCFARLAND. As far as the word "dangerous," I probably didn't use that.

Mr. CUMMINGS. But, I mean, you told her the urgency of the moment.

Mr. MCFARLAND. Absolutely.

Mr. CUMMINGS. And the problems that we are having and where you see it heading.

Mr. MCFARLAND. Yes, in a letter.

Mr. CUMMINGS. Well, come on now.

Ms. ARCHULETA. He sent a letter attached to the flash audit. And we have not had the opportunity to sit down with him. And I take very seriously his concerns, Mr. Cummings. And the opportunity, if he uses the word "dangerous," I need to understand clearly from him and his staff why he attaches that word. And the flash audit needs the scrutiny of both him and I together to protect the employees and to protect our data, to protect our systems.

Chairman CHAFFETZ. Ms. Archuleta, with all due respect, and I know you are fairly new to this position, but the audits have been coming from the Inspector General's Office since 1997. They come year in and year out. They have happened and happened and happened and happened. I mean, I started the other hearing by reading through all the comments that have come along.

So this is a flash audit. You haven't had time to talk about it. You haven't had time to go through it. And yet you can award a multimillion dollar contract in less than 48 hours. That's what we don't understand. And we are going to go through that here in a minute. We are almost done with this hearing. But this isn't just one audit. This isn't just one observation. The good people in the Inspector General's Office have been warning about this since the 1990s. And it was never taken care of.

Ms. ARCHULETA. Thank you for pointing that out. And I appreciate it and acknowledge that.

I have been here 18 months, and I took seriously the audits that came before me. And that is why I have done and taken the steps.

Chairman CHAFFETZ. We don't believe you. I think you are part of the problem. I think if we want different results, we are going to have to have different people. And if you want to refresh the deck, and we want to put Mr. Ozment or somebody else in charge like that, let's to it because you know what, we got a crisis. That hurricane has come and blown this building down. And I don't want to hear about putting boards up on windows, and it's going to take years to get there. That's why I think it's time for you to go.

And, Ms. Seymour, I am sorry, but I think you are in over your head. And I think the seriousness of this requires new leadership and a new fresh set of eyes to do that. I wish you both the best in life. I am not out here to get you. But you know what, this is as big as it gets. And there are going to have to be a new team brought in. That's where I am at on this.

Yield back to the gentleman.

Mr. CUMMINGS. I yield back.

Chairman CHAFFETZ. I am going to recognize myself.

We have got to talk about some things.

Mr. Hess, have you come up with a decision about the timing of when you will provide this information I asked for previously?

Mr. HESS. You will have it by next week.

Chairman CHAFFETZ. Fair enough. Next week, if we can get that information, we would certainly appreciate it. And we will follow up. I will follow up.

Chairman CHAFFETZ. I got Mr. Cummings' back on this one, and I will support him in this. He is asking reasonable questions. And I appreciate the cooperation. Thank you.

I am going to yield to the gentleman from Alabama, who has brought up a great issue and a great point. And I want to go through this contract timeline here again. We are getting close to wrapping up. But, on Thursday, May 28 of this year, just not too long ago, at 11:33 a.m., OPM posted a 29-page request for quotes to provide notification, credit report access, credit monitoring, identity theft insurance, and recovery service, and project management services.

On May 28, 2015, at 1:46 p.m., OPM posted amendment 1, a pricing sheet. On May 29, at 1:32 p.m., OPM changed the deadline from May 20 to May 30. On May 29, at 2:45 p.m. OPM posted another change, modified info to be submitted, and deleted some of the clauses. And, on Tuesday, June 2, a contract was Winvale Group. I don't know the Winvale Group. Could be nice people. I don't know.

But they immediately turned around and subcontracted this to a group I don't know a whole lot about. I want to have Mr. Palmer ask you some questions about this.

Mr. PALMER. Thank you, Mr. Chairman.

This question is to you, Ms. Seymour. Do you know any of the management of CSID?

Ms. SEYMOUR. Not that I am aware of, sir.

Mr. PALMER. Do you know or have any knowledge about the management of CSID?

Ms. SEYMOUR. No, sir, not that I am aware of. I got key personnel resumes in the proposals.

Mr. PALMER. Did anyone discuss with you any knowledge about the CEO Scott Cruickshank? He is the chairman of the board.

Ms. SEYMOUR. No, sir.

Mr. PALMER. About Hazem Ben-Gacem?

Ms. SEYMOUR. No, sir.

Mr. PALMER. How about James Mansour?

Ms. SEYMOUR. No, sir.

Mr. PALMER. There are only four directors. So the last one is Owen Li. I asked you about him earlier.

Ms. SEYMOUR. No, sir. I have no recollection of them.

Mr. PALMER. You know, you let a contract in a very sensitive area. I mean, this literally impacts millions of people. It potentially impacts their financial well-being, their careers, yet it appears that you didn't do the most basic research into the company that you have contracted this with. If you had, I think you might have discovered that Mr. Li is under investigation by the Department of Justice and the Securities and Exchange Commission. They are looking into his management of a group called Canarsie, in which

in 9 months, he lost 99.7 percent of the money invested in that hedge fund.

Mr. McFarland, let me ask you this. If you had known this, would this have raised a red flag with the Inspector General's Office?

Mr. MCFARLAND. Absolutely.

Mr. PALMER. I have listened to Mr. Cummings. I have listened to the chairman. And the more I listen to these guys and the members of this entire committee ask these questions, the more concerned and more frightened I have become about how OPM has handled this. And then to find this and to find that just the most basic analysis has not been done just adds to that.

One other question I want to ask you. Mr. Ozment, who testified last week, made this comment. I want to ask you, are you aware of any outside contractors who are foreign nationals? Have you contracted any work with them?

Ms. Seymour?

Ms. SEYMOUR. I am sorry, I didn't realize that was my question. I apologize. Am I aware of any——

Mr. PALMER. Have you contracted any of this work to foreign nationals?

Ms. SEYMOUR. Not that I am aware of, sir.

Mr. PALMER. How about you, Ms. Archuleta?

Ms. ARCHULETA. No, sir.

Mr. PALMER. May I read this? Or do you want to read it? This is from the Wall Street Journal. This is Mr. Ozment. He said: Some of the contractors that have helped OPM with managing internal data have had security issues of their own, including potentially giving foreign governments direct access to the data long before the recent reported breaches. A consultant who did some work with the company contracted by OPM to manage personnel records for a number of agencies told ARS that he found the Unix systems administrator for the project was in Argentina, and his coworker was physically located in the People's Republic of China. Both had direct access to every row of data and every database. They were root. Another team that worked with these databases had at its head it two teams members with Republic of China passports—People's Republic of China passports. I know that because I challenged and personally revoked the privileges.

You are not aware of that?

Ms. SEYMOUR. Sir, I am aware of two of our—two Federal employees who have ties to foreign countries. They are U.S. citizens, and they work on our programs.

Mr. PALMER. How are they—does it not raise—here is what Ozment said. He said from his perspective, OPM compromised this information more than 3 years ago. And his take on the current breach is, so what is new?

I yield the balance of my time.

Chairman CHAFFETZ. I would like to ask unanimous consent to enter into the record this article. This is written by Julia La Roche. It is March 27, 2015, "Hedge Fund Manager Who Said Sorry for Losing 99.7 Percent of His Client's Money is Now Being Investigated By the SEC and the Department of Justice."

Ms. Seymour, were you aware that the contract that you let for Winvale was going to be sublet, or there would be a subcontractor?

Without objection, by the way, I will enter this article into the record.

Chairman CHAFFETZ. Did you know that there was going to be a subcontract?

Ms. SEYMOUR. Winvale's proposal included the fact that it had work—that it was subcontracting or partnering with CSID on it.

Chairman CHAFFETZ. So when you did your due diligence and you looked into some of the resumes of the people that would be involved and engaged in this, did that include the employees and the board at this subcontractor?

Ms. SEYMOUR. It did not include the board. We used past performance, and there are other systems that the contracting officer uses to research a firm to make sure that they are qualified to do work with the Federal Government.

Chairman CHAFFETZ. Had either Winvale or the subcontractor, or if there is more than one subcontractor, do you personally know anybody who is in any way, shape, or form involved in any of those companies?

Ms. SEYMOUR. Not to my knowledge, sir.

Chairman CHAFFETZ. There is nobody from the former Department of Defense or from the Office of Personnel Management? You know none of those people?

Ms. SEYMOUR. I do not believe I know anyone that's working for those firms.

Chairman CHAFFETZ. Ms. Archuleta, do you know anybody that works for either of those two firms?

Ms. ARCHULETA. Not to my knowledge.

Chairman CHAFFETZ. So here we have somebody who lost millions of dollars, under investigation by the Department of Justice. We have got to figure out how in the world these people get the contract because now what we are doing is we are saying: Okay, all you Federal employees, millions of you that were affected, go give them your information.

And that's the kind of person we are dealing with. I am not saying he is guilty. But he is under investigation. Why should we take the chance? Why didn't you go to the GSA list? I mean, there is a list of approved vendors out there. Why not use one of them?

Ms. SEYMOUR. We did consult with GSA and the GSA schedule on this. There were some requirements that we wanted to include in our contract that were not available on the GSA schedule.

Chairman CHAFFETZ. Like what?

Ms. SEYMOUR. D duplication of services is one of them. What we were trying to do at OPM was to set up a contract vehicle that we could use in the future for any additional breaches, whether it's one or twosies or anything else. We wanted to set up a vehicle that would not cause us to pay or to offer the same services to affected individuals at the same time. That is not something that the GSA schedule afforded us the opportunity to do, even after we talked with the schedule holder at GSA.

Chairman CHAFFETZ. I am just telling you, this reeks. And for any contract to go out that fast, I understand the gravity of this situation, you are going to deviate from that and then they imme-

diately go out to subcontract, I would encourage you to as swiftly as possible get back to Senator Warner and Mr. Palmer as well as this committee.

I do need to ask about credentials. Ms. Archuleta, is there anybody in the OPM system, whether they be an employee or a contractor, who is a foreign national?

Ms. ARCHULETA. Sir, I want to be sure of that answer. I would have to come back to you to be sure that I——

Chairman CHAFFETZ. Ms. Seymour, is there anybody who is a foreign national who is involved as either a contractor or directly as an employee at OPM?

Ms. SEYMOUR. I will get back to you on that, sir.

Chairman CHAFFETZ. The fact that you two don't know, that's what scares me. That's what really scares me is that you don't know.

Ms. SEYMOUR. I know about my staff, sir.

Chairman CHAFFETZ. How many people on your staff?

Ms. SEYMOUR. About 280.

Chairman CHAFFETZ. How many people have credentials to become a network administrator or have access to the network? How many?

Ms. SEYMOUR. I believe it is about 50.

Chairman CHAFFETZ. So of those 50 people—and how often do you routinely audit that?

Ms. SEYMOUR. We review them very frequently.

Chairman CHAFFETZ. Like what?

Ms. SEYMOUR. Probably monthly. We have processes for when people come onboard and when they leave, that we remove their access privileges.

Chairman CHAFFETZ. Do you review the traffic that's going through there? Because that's evidently part of what happened is somebody gained network administrator access and——

Ms. SEYMOUR. So that's how we were able to track through and understand that our background investigations——

Chairman CHAFFETZ. After they had been there for than a year, right?

Ms. SEYMOUR. Yes, sir.

Chairman CHAFFETZ. So how often do you track that and monitor that?

Ms. SEYMOUR. So we had put the tools on our network just over the last 6 months or so to be able to see this type of activity in our network. Again, sir, when I came on board, I recognized that these systems were in need of some modernization. We put in place a plan and began to execute that immediately to put the security tools in place so that we had visibility in our network. That's what led us to understand this latent activity that went back to even prior to my arrival at OPM.

Chairman CHAFFETZ. I have got a series of other questions, but let's recognize the gentleman from Georgia, Mr. Carter, for 5 minutes.

Mr. CARTER. Thank you, Mr. Chairman.

And thank all of you for being here.

Ms. Seymour, I would like to start with you. It's my understanding that OPM's legacy system, that you are currently using

COBOL, a system that was developed originally in 1959, is that correct?

Ms. SEYMOUR. I don't know when it was invented, sir, but yes, we are using COBOL in some of our systems at OPM.

Mr. CARTER. Okay. According to my research and my staff research, it was originally developed in 1959. And that's the system that we are using?

Ms. SEYMOUR. Yes, sir.

Mr. CARTER. Ms. Archuleta, OPM since 2008 has spent $577 million on IT. Is that correct?

Ms. ARCHULETA. I don't know exactly that number, but I will accept that.

Mr. CARTER. You think that's pretty close?

Ms. ARCHULETA. I would have to trust your judgment. I don't know that number yet, but I could get back to you. But yes, if you want to——

Mr. CARTER. But would you say that's in the ballpark, $577 million? I mean, give or take a couple hundred million, what are we talking about?

Ms. ARCHULETA. I can tell you what we spent on it, but yes, I will——

Mr. CARTER. $577 million dollars since 2008, yet we are still using a legacy system that was developed in 1959?

Ms. ARCHULETA. I agree with you totally, sir. We are using a legacy system that was designed in 1959. And that is what we are working to change.

Mr. CARTER. It's my understanding that approximately 80 percent of our IT budget is being spent on legacy systems. Is that correct?

Ms. ARCHULETA. Right now, we are working off of our legacy system. That's why we are making the investments into a new system.

Mr. CARTER. I am sorry, I am just flabbergasted by this. It's just mind-boggling that we can spend—first of all, we can spend $577 million; secondly, that we are spending 80 percent of what we have budgeted on legacy systems. I mean, it's just amazing to me that we're doing that.

Nevertheless, Ms. Seymour, let me ask you, the IG's flash audit indicated that the estimated cost for just two phases, only two phases of your infrastructure improvement project, is going to be $93 million. Is that correct?

Ms. SEYMOUR. Yes, sir. We put together the plan with a very robust interagency team and had that reviewed by a number of experts.

Mr. CARTER. $93 million?

Ms. SEYMOUR. Yes, sir.

Mr. CARTER. I am sorry, I don't mean to be dramatic, but $93 million?

Ms. SEYMOUR. That covers both securing our legacy architecture, the one that we have today——

Mr. CARTER. The one that was originally developed in 1959?

Ms. SEYMOUR. Not all of it was developed that long ago.

Mr. CARTER. If any of it was developed.

Ms. SEYMOUR. So our network was designed, you know, about a decade ago. So we are trying to shore that up, provide as much se-

curity around that network as we can. That's part of what the money is going to. And then the other part of the money is going towards building a more modern and more securable network that we will transition to.

Mr. CARTER. Okay. Okay. Well, it's my understanding that despite the decades that we have been spending all this money, these millions of dollars, that we are still using paper forms in some cases? Is that true?

Ms. SEYMOUR. A number of our business offices still use paper forms.

Mr. CARTER. We have spent $577 million on IT since 2008, and we are still using paper forms. Of course, hey, paper forms may be better in this case. I mean, at least we have still got control of those.

Ms. SEYMOUR. I can't speak to what's happened before me, sir. I can tell you that when I came in and saw the state of our IT systems, I worked with Director Archuleta to put in place a plan, an aggressive plan, for migrating to more modern, more secure network and systems.

Mr. CARTER. Does it include paper forms? Does it include paper forms? Will we still have paper forms after you make these adjustments?

Ms. SEYMOUR. We want to remove as much paper as we can from our environment, sir. That's one of our goals.

Mr. CARTER. I can't help but wonder if that's not a move in the wrong direction. At least we can have some control over these paper forms. We obviously don't have control over the computers and the information that we have on the Internet.

Ms. SEYMOUR. I would offer, sir, that there are security concerns with paper just as well. We have, you know, violations or issues with paper as well as you leave paper around. The other issue we have with paper, sir——

Mr. CARTER. So we leave paper around?

Ms. SEYMOUR. Sir, when you leave it in your office or when you are working with it. I would also offer that when we have paper, we don't have backup systems. That's a concern as well as we move forward with our automated——

Mr. CARTER. Ms. Seymour, I agree with every point you are making here. My point is that we spent $577 million since 2008, and we are still using paper.

Ms. SEYMOUR. And, sir, I also said I can't tell you what has gone on before me. What I can tell you is the plan we are putting in place, we are planning to put in place an enterprise case management system. We are working towards that. That will eliminate a lot of our paper. We will modernize our systems and provide better protections around our data and our systems.

Mr. CARTER. And that includes that $577 million that we have already spent?

Ms. SEYMOUR. I am sorry, sir?

Mr. CARTER. This is going to be more money we are going to throw at this problem, right?

Ms. SEYMOUR. Again, sir, I cannot account for what has happened before me.

Chairman CHAFFETZ. Thank the gentleman.

We have a vote on the floor. I will recognize Mr. Cummings, who has got a few more questions.

Mr. CUMMINGS. I will be very quick, Mr. Chairman. Thank you very much. I want to go back to this contract. Winvale got this contract. Is that right, Ms. Seymour?

Ms. SEYMOUR. Yes, sir, that's correct.

Mr. CUMMINGS. What was the process? It doesn't smell right. Something doesn't smell right about this contract. Winvale gets it, and then they turn around and CSID, what?

Ms. SEYMOUR. No, sir. The proposal that we got was from Winvale partnered with CSID. We knew up front that they were—they had support from CSID. It was part of their proposal package to the government.

Mr. CUMMINGS. And you didn't know about Mr. Li?

Ms. SEYMOUR. No, sir, I did not.

Mr. CUMMINGS. You didn't know of his apology for losing 99.7 percent of $60 million went viral?

Ms. SEYMOUR. No, sir, I did not.

Mr. CUMMINGS. In March?

Ms. SEYMOUR. No, sir, I did not.

Mr. CUMMINGS. And so the question becomes—I mean, do you think you should have done some better due diligence?

Ms. SEYMOUR. So we did due diligence on the company. There are several ways that the contracting officer validates that the company is able to do business with the government.

Mr. CUMMINGS. And, Mr. McFarland, this concerns you I take it.

Mr. MCFARLAND. Yes, of course.

Mr. CUMMINGS. And why is that, sir?

Mr. MCFARLAND. Just because of the reasons that you have espoused. It was very fast. And as a matter of fact, a few days ago, we were talking about that in the office. And we are going to be looking into it.

Mr. CUMMINGS. I appreciate that. I just have one statement real quick, Mr. Chairman. I want to conclude by thanking you again for agreeing to invite the contractors here today. We have obtained some significant information. But there are also many, many unanswered questions. We asked USIS for information they have refused to give us for more than a year. Mr. Giannetta promised to help us get those answers. But I am concerned that he may not be there in a couple weeks. So we may need to follow up with USIS' parent company, Altegrity.

We also asked KeyPoint for documents we originally requested months ago. And you pressed them to provide those documents. I think you understand how frustrating it has been for me over the past year. So I thank you for your help, for agreeing to invite them, for helping us get the information we need. We will prepare questions for the record for today. And I hope we will be able to get all of these answers. And I really do hope it won't require a subpoena.

With that, I thank you, and I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We are now at the halfway point. I am just teasing. We are wrapping up here. We are wrapping up. You all have been sitting here for a long time. All right. So a couple more questions. We do have votes on the floor.

Director Archuleta, I need to go back to some of your previous comments. This has to do with what you said in July of 2014 regarding the OPM data breach that became public in March of that year. At the time, you said that you did not have a breach in security. Ms. Seymour was very candid in saying that she did think it was a breach in security. So is she wrong?

Ms. ARCHULETA. As I explained earlier, sir, in the question that was asked me, the conversation was around PII, and I answered it in that context.

Chairman CHAFFETZ. But you don't believe there was any access to see that information?

Ms. ARCHULETA. I don't believe that there was—that that data was breached and that there was no data exfiltrated.

Chairman CHAFFETZ. Exfiltrated. But do you believe that they had at least access to it to look at it?

Ms. ARCHULETA. That's why we understand that there was in fact a breach. I am not the forensics. I don't know what they did with it. What I was assured of, sir, and why I responded in that interview was there was no PII extricated from the system.

Chairman CHAFFETZ. So you did know that the OPM network, the network platform, that the blueprint, essentially the keys to the kingdom, was exfiltrated, right? You did know that.

Ms. ARCHULETA. As I said, the question was around the PII, and that's the way I answered it.

Chairman CHAFFETZ. I am asking you now. I am asking you now, do you believe—you knew, somehow you had to know, I hope.

Ms. ARCHULETA. Ms. Seymour informed me that other data had been taken from, but it was not—it was in different context to that question.

Chairman CHAFFETZ. But that was essentially a blueprint of how the system worked. Correct?

Ms. ARCHULETA. She had informed me that some manuals had also been exposed and potentially exfiltrated, yes. I knew that. Again, in that interview, the question was around PII.

Chairman CHAFFETZ. Okay. So but you did know that there was a security breach. Correct?

Ms. ARCHULETA. Correct.

Chairman CHAFFETZ. And you did know that there were things other than the PII that were potentially exfiltrated. Correct?

Ms. ARCHULETA. I did.

Chairman CHAFFETZ. You did know that.

What do you think is a bigger success for hackers, you know, stealing the files for tens of thousands of employees or the files for 32 million, up to 32 million employees?

Ms. ARCHULETA. I believe that all of that is very important, sir. I can't distinguish between both of them. They are each equally as important.

Chairman CHAFFETZ. So when did the hackers first gain access to OPM's network? The ones we just learned about? Maybe Ms. Seymour is in a better position to answer that. Either one of you. If you know what the timeline is on that.

Ms. BARRON-DICAMILLO. I have the timeline associated with that, sir.

Chairman CHAFFETZ. Yes.

Ms. BARRON-DiCAMILLO. So the actors first gained—adversary access was first noted within the network around November of 2013.

Chairman CHAFFETZ. The ones that we just learned about?

Ms. BARRON-DiCAMILLO. I am sorry, that was from the 2014 intrusion that you were referencing based upon the manuals.

Chairman CHAFFETZ. I am sorry, that happened in what timeframe?

Ms. BARRON-DiCAMILLO. We were able to confirm, based upon the onsite assessment, that they had access, confirmed access in November of 2013.

Chairman CHAFFETZ. Okay. Ms. Seymour, I think you were going to say something.

Ms. SEYMOUR. I was just going to try clarify for you, sir, that for this most recent incident, it dates backs to June of 2014. The access that the adversary had dates back to June of 2014, I believe.

Chairman CHAFFETZ. Is it possible that when they took this blueprint—I call it the keys to the kingdom—that that would have potentially aided the hackers in coming back into the system and stealing these millions of records?

Ms. SEYMOUR. These are available manuals typically for commercial IT equipment. So, yes, it would aid an adversary in understanding our platform. They did not get, you know, specific configuration diagrams of our entire environment. But these are commercially available—a lot of these are commercially available documents about platforms, computing platforms.

Chairman CHAFFETZ. Ms. Barron-DiCamillo, did they include any proprietary information, anything that was——

Ms. BARRON-DiCAMILLO. Based on what we saw as the potential exfil, it did not include proprietary information or specific information around the architecture of the OPM environment. It was manuals associated with certain types of platforms. But, again, as Ms. Seymour stated, a lot of that information is also publicly available. It's available on—I think IBM is one of the——

Chairman CHAFFETZ. Did the hackers have access to be able to see the information regarding personal employees?

Ms. BARRON-DiCAMILLO. So, in 2014, is that the incident you are referring to?

Chairman CHAFFETZ. Yes.

Ms. BARRON-DiCAMILLO. So based on the onsite assessment, we weren't able to confirm that they were able to access any of the PII information. So not only so your question about seeing it, they did not—there is certain portion of the network they were specifically focused on, and they were not able to infiltrate into those portions of the network.

Chairman CHAFFETZ. Ms. Seymour—or let me ask Ms. Archuleta. If Ms. Seymour was responsible for safeguarding the PII, as we call it, information in 2014, who do you hold responsible for its loss today?

Ms. ARCHULETA. I hold all of us responsible. That's our job at the OPM. We work very hard to do this, and we work with our partners across government. I know that you are perhaps tired of hearing this from me, but we are facing a very aggressive attacker. We protect against 10 million attempts each month. So we are working

very hard to do that. We are working extremely hard to prevent the types of things that we are seeing here today.

Chairman CHAFFETZ. Mr. Cummings.

Mr. CUMMINGS. Mr. Hess, I want to make sure you are going to get us some documents. We have been requesting documents a long time. I want to make sure what documents you are going to provide us. Are those the ones we have been asking for?

Mr. HESS. We are going to be addressing——

Mr. CUMMINGS. I can't hear you.

Mr. HESS. I am sorry. We are going to be addressing that letter and each of the requests that you made to the extent that we are able to.

Mr. CUMMINGS. All right. Thank you.

Chairman CHAFFETZ. It's been a long morning and into the afternoon. I thank you all. You all represent a number of people that have a lot of staff, people who work hard. They are patriotic. They care about this country. To that extent, please let them know how much we appreciate them and all that you are doing. But we will have somebody help you know where the restroom is. It's been a while.

So, again, thank you for your participation today. We stand adjourned.

[Whereupon, at 1:54 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION
1100 Connecticut Avenue NW • Suite 900 • Washington, DC 20036
Phone: 202-293-1550 • www.fleoa.org

Representing Members Of:
AGRICULTURE
OIG
Forest Service
COMMERCE
Export Enforcement
OIG
NOAA Fisheries Law Enforcement
DEFENSE
Air Force – OSI
Army – CID
Defense Criminal Investigative Service
Naval Criminal Investigative Service
OIG
EDUCATION – OIG
ENERGY
National Nuclear Security Administration
OIG
ENVIRONMENTAL PROTECTION AGENCY
CID
OIG
FEDERAL DEPOSIT INSURANCE CORPORATION – OIG
GENERAL SERVICES ADMINISTRATION – OIG
HEALTH AND HUMAN SERVICES
OIG
Food and Drug Administration
HOMELAND SECURITY
Border Patrol
Coast Guard Investigative Service
Immigration and Customs Enforcement
Customs and Border Protection
Federal Air Marshal Service
Federal Emergency Management Agency
Federal Protective Service
U.S. Secret Service
Transportation Security Administration
OIG
HOUSING AND URBAN DEVELOPMENT – OIG
INTERIOR
Bureau of Indian Affairs
Bureau of Land Management
Fish and Wildlife Service
National Park Service
OIG
U.S. Park Police
JUSTICE
Bureau of Alcohol, Tobacco, Firearms and Explosives
Drug Enforcement Administration
Federal Bureau of Investigation
Federal Air Marshal Service
OIG
U.S. Attorney's Office – CI
LABOR – OIG
POSTAL SERVICE
Postal Inspection Service
OIG
SOCIAL SECURITY ADMINISTRATION – OIG
STATE DEPARTMENT
Bureau of Diplomatic Security
OIG
TRANSPORTATION – OIG
TREASURY
FinCEN
OIG
Internal Revenue Service – CI
TIGTA
U.S. CAPITOL POLICE
U.S. PROBATION AND PRETRIAL SERVICES
VETERANS AFFAIRS
OIG
VA Police
RETIREES

June 16, 2015

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Chaffetz, Chairman Johnson, Ranking Member Cummings, and Ranking Member Carper:

The Federal Law Enforcement Officers Association (FLEOA) is the largest non-partisan professional association that exclusively represents over 28,000 current and retired federal law enforcement officers and special agents from over 65 federal agencies.

Below are FLEOA's concerns about the Office of Personnel Management (OPM) data breaches, our demands of the government, and a list of questions that remain unanswered.

1. OPM turned its back on Federal Law Enforcement Officers (LEOs) when they failed to protect sensitive information from an inexcusable breach, and OPM's delayed and aloof response is a pathetic and irresponsible miscarriage of its obligations to affected Americans.
2. The very lives of federal Law Enforcement Officers (LEOs) are now in danger, and the safety and security of innocent people—including LEO families—are now in jeopardy because of OPM's abysmal failure and its continuing ignorance of the severity of the breach.
3. The information lost includes personal, financial and location information of LEOs and their families leaving them vulnerable to attack and retaliation from criminals and terrorists currently or formerly investigated by the United States.

4. If one LEO or a family member is harmed or killed, OPM will have blood on their hands.
5. The information lost can lead to the theft of additional information on tens or hundreds of millions of Americans, and thousands of foreign nationals who do business with the United States.
6. OPM's failure threatens the lives of covert operatives and agents. In addition, this kind of information often is used to spy on or steal information against the United States.

FLEOA Demands:

1. FLEOA demands a full investigation by the FBI and other authorities external to OPM, with the possibility of criminal charges and civil lawsuits arising from its findings.
2. FLEOA demands that OPM provide long-term virtual and physical protections for those in danger, including lifetime credit and other monitoring to detect and prevent attacks by international adversaries, criminals and terrorists.
3. FLEOA demands an immediate overhaul of the security system used to store and access sensitive information, including firewalls, separate servers, proper authentication, and other state-of-the-art technology.
4. FLEOA demands immediate answers on exactly what information was breached so that LEOs can protect themselves.

Unanswered questions for OPM:

1. Exactly what information was stolen?
2. What is OPM going to do to provide for the safety and security of LEOs and their families now that their lives and financial security are in jeopardy?
3. When LEO's are at work, how will OPM keep their families safe?
4. Will OPM cover the costs or indemnify the individuals who suffer harm if their identity is stolen (employees, family, friends and others listed on stolen forms)?
5. It is illegal to release or improperly secure information. Who will be held accountable?
6. Why did OPM allow highly sensitive information accessible via an internet connection, without secure, separate servers and firewalls to protect employees?
7. There are a number of criminal justice information services that are completely accessible by its users but have never been breached because they are properly protected and firewalled. Why is OPM not using this strategy for some of the country's most sensitive information?

FLEOA appreciates the attentiveness of lawmakers and the House and Senate oversight committees to our unique concerns regarding officer safety and the safety of our families.

Sincerely,

Jon Adler

Jon Adler
FLEOA National President

CC: The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform
The Honorable Thomas Carper, Ranking Member, Senate Homeland Security and Governmental Affairs Committee

The Washington Post

In the Loop

Defense firm that employed drunk, high contractors in Afghanistan may have wasted $135 million in taxpayer dollars

By Colby Itkowitz May 13

The defense contractor investigated in 2012 after cellphone videos surfaced of its employees drunk and high on drugs in Afghanistan may have misused almost $135 million of U.S. taxpayer money, an audit finds.

A financial audit done on behalf of the independent Special Inspector General for Afghanistan Reconstruction (SIGAR) alleges Arlington-based Imperatis Corporation, formerly Jorge Scientific Corporation, couldn't produce documents to show whether some payments to a subcontractor were allowed under its contract with the Army.

The IG report, released in April, said either Imperatis should produce the appropriate documents "to demonstrate that the costs invoiced and paid were allowable..." or refund the money to government.

Sens. Claire McCaskill (D-Mo.) and Rob Portman (R-Ohio), the ranking Democrat and chairman, respectively, of the Senate Homeland Security and Governmental Affairs subcommittee on investigations, are now demanding a full briefing from the Army Contracting Command about all its contracts with Imperatis, which over time have totaled nearly $1 billion.

In a letter Tuesday to the agency's Commanding General Theodore Harrison, McCaskill and Portman highlighted the previous issues with the firm after which, they wrote, the company assured them it "had taken action to ensure that there was no further misconduct by Jorge Scientific employees in Afghanistan."

"After allegations of frequent drug and alcohol abuse, bar brawls, and out-of-control parties among its employees in Afghanistan, this contractor is now facing additional scrutiny into its business practices to the possible tune of more than $130 million in taxpayer dollars, and we intend to get to the bottom of it," McCaskill said in an e-mail to the Loop.

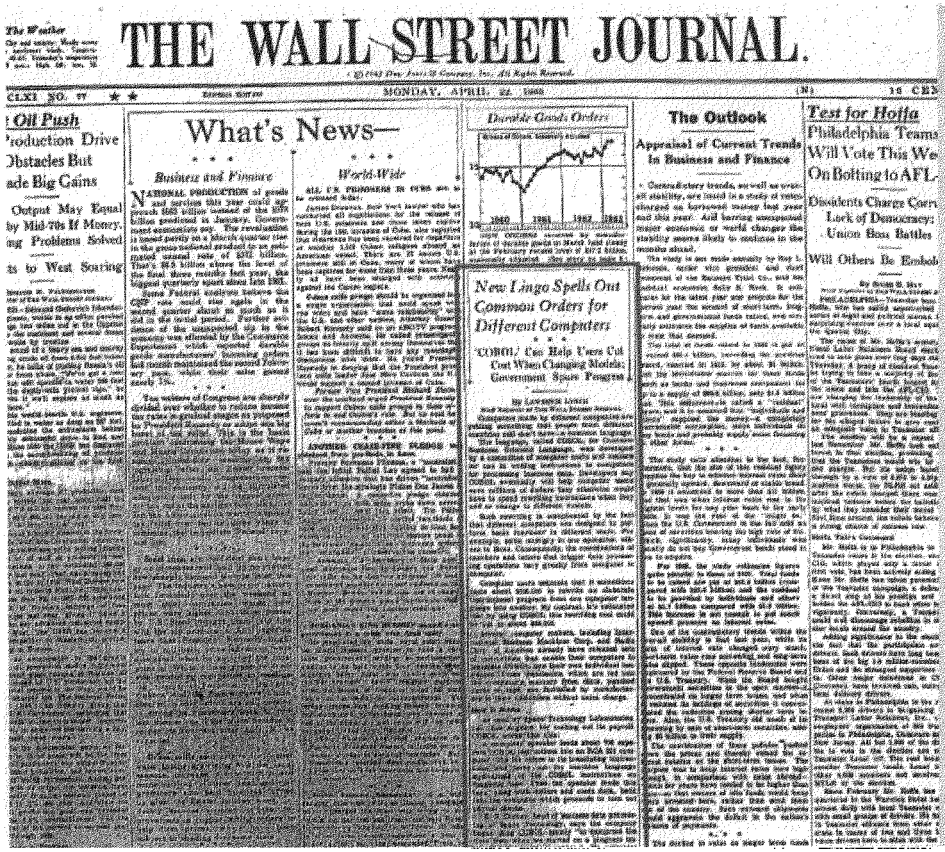
The Army uses Imperatis to provide counterinsurgency intelligence training for Afghan security forces through its Legacy Easy Project. In 2012, two former employees filed a complaint that there was rampant use of drugs and alcohol by then-Jorge Scientific personnel in Afghanistan. They took cellphone video of wasted employees that they gave to ABC News, which first reported the story.

After that story broke, McCaskill wrote to Secretary of the Army John McHugh asking for a review of Jorge Scientific's contracts. She received a response that the Army was looking into it, and had subsequent briefings. She was assured everyone involved had been fired and there would be more oversight.

Imperatis has responded forcefully to the recent independent audit, asking that the findings be reconsidered or that SIGAR "provide more time and funding to complete the audit."

More funding?

Colby Itkowitz is a national reporter for In The Loop.



THE WALL STREET JOURNAL.

MONDAY, APRIL 22, 1963

What's News—

Business and Finance

World-Wide

Durable Goods Orders

New Lingo Spells Out Common Orders for Different Computers

'COBOL' Can Help Users Cut Cost When Changing Models; Government Spurs Progress

The Outlook

Appraisal of Current Trends In Business and Finance

Test for Hoffa

Philadelphia Teams Will Vote This We On Bolting to AFL

Dissidents Charge Corr Lack of Democracy; Union Boss Battles

Will Others Be Emboli

THE WALL STREET JOURNAL
APRIL 22, 1963

New Lingo Spells Out Common Orders for Different Computers

'COBOL' Can Help Users Cut Cost When Changing Models: Government Spurs Progress

...

The language, called COBOL, for Common Business Oriented Language, was developed by a committee of computer users and makers for use in writing instructions to computers for processing business data. Developers say COBOL eventually will help computer users save millions of dollars they otherwise would have to spend rewriting instructions when they add or change to different models.

...

COBOL's use is limited to such everyday business tasks as turning out payrolls and efficiency reports.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

June 24, 2015

The Honorable Jason Chaffetz
2157 Rayburn House Office Building
Committee on Oversight and Government Reform
United States House of Representatives
Washington, DC 20515

Dear Chairman Chaffetz:

I would like to address the confusion regarding the number of people affected by the two recent, related cyber incidents at the Office of Personnel Management.

First, it is my responsibility to provide as accurate information as I can to Congress, the public, and most importantly, the affected individuals. Second, because this information and its potential misuse concerns their lives, it is essential to identify the affected individuals as quickly as possible. Third, we face challenges in analyzing the data due to the form of the records and the way they are stored. As such, I have deployed a dedicated team to undertake this time-consuming analysis and instructed them to make sure their work is accurate and completed as quickly as possible. As much as I want to have all the answers today, I do not want to be in a position of providing you or the affected individuals with potentially inaccurate data.

With these considerations in mind, I want to clarify some of the reports that have appeared in the press. Some press accounts have suggested that the number of affected individuals has expanded from 4 million individuals to 18 million individuals. Other press accounts have asserted that 4 million individuals have been affected in the personnel file incident and 18 million individuals have been affected in the background investigation incident.

Therefore, I am providing the status as we know it today and reaffirming my commitment to providing more information as soon as we know it.

First, the two kinds of data I am addressing – personnel records and background investigations – were affected in two different systems in two recent incidents. Second, the number of individuals with data compromised from the personnel records incident is approximately 4.2 million, as we reported on June 4, 2015. This number has not changed, and we have notified these individuals. Third, as I have noted, we continue to analyze the background investigation

data as rapidly as possible to best understand what was compromised, and we are not at a point where we are able to provide a more definitive report on this issue.

That said, I want to address the figure of 18 million individuals that has been cited in the press. It is my understanding that the 18 million refers to a preliminary, unverified and approximate number of unique social security numbers in the background investigations data. It is not a number that I feel comfortable, at this time, represents the total number of affected individuals. The Social Security number portion of the analysis is still under active review, and we do not have a more definitive number. Also, there may be overlap between the individuals affected in the background investigation incident and the personnel file incident. Additionally, we are working deliberately to determine if individuals who have not had their Social Security numbers compromised, but may have other information exposed, should be considered individuals affected by this incident. For these reasons, I cannot yet provide a more definitive response on the number of individuals affected by the background investigations data intrusion, and it may well increase from these initial reports. My team is conducting this further analysis with all due speed and care, and again, I look forward to providing an accurate and complete response as soon as possible.

I look forward to addressing any questions you may have.

Sincerely,

Katherine Archuleta

Katherine Archuleta
Director

The New York Times http://nyti.ms/1mATnjr

ASIA PACIFIC

Chinese Hackers Pursue Key Data on U.S. Workers

By MICHAEL S. SCHMIDT, DAVID E. SANGER and NICOLE PERLROTH JULY 9, 2014

WASHINGTON — Chinese hackers in March broke into the computer networks of the United States government agency that houses the personal information of all federal employees, according to senior American officials. They appeared to be targeting the files on tens of thousands of employees who have applied for top-secret security clearances.

The hackers gained access to some of the databases of the Office of Personnel Management before the federal authorities detected the threat and blocked them from the network, according to the officials. It is not yet clear how far the hackers penetrated the agency's systems, in which applicants for security clearances list their foreign contacts, previous jobs and personal information like past drug use.

In response to questions about the matter, a senior Department of Homeland Security official confirmed that the attack had occurred but said that "at this time," neither the personnel agency nor Homeland Security had "identified any loss of personally identifiable information." The official said an emergency response team was assigned "to assess and mitigate any risks identified."

One senior American official said that the attack was traced to China, though it was not clear if the hackers were part of the government. Its disclosure comes as a

delegation of senior American officials, led by Secretary of State John Kerry, are in Beijing for the annual Strategic and Economic Dialogue, the leading forum for discussion between the United States and China on their commercial relationships and their wary efforts to work together on economic and defense issues.

Computer intrusions have been a major source of discussion and disagreement between the two countries, and the Chinese can point to evidence, revealed by Edward J. Snowden, that the National Security Agency went deep into the computer systems of Huawei, a major maker of computer network equipment, and ran many programs to intercept the conversations of Chinese leaders and the military.

American officials say the attack on the Office of Personnel Management was notable because while hackers try to breach United States government servers nearly every day, they rarely succeed. One of the last attacks the government acknowledged occurred last year at the Department of Energy. In that case, hackers successfully made off with employee and contractors' personal data. The agency was forced to reveal the attack because state disclosure laws force entities to report breaches in cases where personally identifiable information is compromised. Government agencies do not have to disclose breaches in which sensitive government secrets, but no personally identifiable information, has been stolen.

Just a month ago, the Justice Department indicted a group of Chinese hackers who work for the People's Liberation Army Unit 61398, and charged them with stealing corporate secrets. The same unit, and others linked to the P.L.A., have been accused in the past of intrusions into United States government computer systems, including in the office of the secretary of defense.

But private security researchers say the indictments have hardly deterred the People's Liberation Army from hacking foreign targets, and American officials are increasingly concerned that they have failed in their effort to deter computer attacks from China or elsewhere. "There's no price to pay for the Chinese," one senior intelligence official said recently, "and nothing will change until that changes."

The indictments have been criticized as long on symbolism and short on real punishment: There is very little chance that the Chinese military members would

ever see the inside of an American courtroom, even if the F.B.I. has put their pictures on wanted posters.

"I think that it was speaking loudly and carrying a small stick," said Dennis Blair, the former director of national intelligence during President Obama's first term, who was a co-author of a report last year urging that the United States create a series of financial disincentives for computer theft and attacks, including halting some forms of imports and blocking access to American financial markets.

Not long after several members of Unit 61398 were indicted, security researchers were able to pin hundreds more cyberattacks at American and European space and satellite technology companies and research groups on a second Shanghai-based Chinese military unit, known as Unit 61486. Researchers say that even after Americans indicted their counterparts in Unit 61398, members of Unit 61486 have shown no signs of scaling back.

The same proved true for the dozen other Chinese military and naval units that American officials have been tracking as they break into an ever more concerning list of corporate targets including drone, missile and nuclear propulsion technology makers.

The intrusion at the Office of Personnel Management was particularly disturbing because it oversees a system called e-QIP, in which federal employees applying for security clearances enter their most personal information, including financial data. Federal employees who have had security clearances for some time are often required to update their personal information through the website.

The agencies and the contractors use the information from e-QIP to investigate the employees and ultimately determine whether they should be granted security clearances, or have them updated.

A representative of the Office of Personnel Management said that monitoring systems at the Department of Homeland Security and the agency office allowed them to be "alerted to a potential intrusion of our network in mid-March."

In the past, the Obama administration has urged American companies to share intrusion information with the government and reveal breaches to consumers in cases where their personal information was compromised and could be used without authorization.

But in this case there was no announcement about the attack. "The administration has never advocated that all intrusions be made public," said Caitlin Hayden, a spokeswoman for the Obama administration. "We have advocated that businesses that have suffered an intrusion notify customers if the intruder had access to consumers' personal information. We have also advocated that companies and agencies voluntarily share information about intrusions."

Ms. Hayden noted that the agency had intrusion-detection systems in place and notified other federal agencies, state and local governments about the attack, then shared relevant threat information with some in the security industry. Four months after the attack, Ms. Hayden said the Obama administration had no reason to believe personally identifiable information for employees was compromised.

"None of this differs from our normal response to similar threats," Ms. Hayden said.

Michael S. Schmidt and David E. Sanger reported from Washington, and Nicole Perlroth from San Francisco. Richard A. Oppel Jr. contributed reporting from New York.

A version of this article appears in print on July 10, 2014, on page A1 of the New York edition with the headline: Chinese Hackers Pursue Key Data on U.S. Workers.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

June 17, 2015

MEMORANDUM FOR KATHERINE ARCHULETA
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055)

Executive Summary

The U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) is issuing this Flash Audit Alert to bring to your immediate attention serious concerns we have regarding the Office of the Chief Information Officer's (OCIO) infrastructure improvement project (Project).[1] This Project includes a full overhaul of the agency's technical infrastructure by implementing additional information technology (IT) security controls and then migrating the entire infrastructure into a completely new environment (referred to as Shell).

Our primary concern is that the OCIO has not followed U.S. Office of Management and Budget (OMB) requirements and project management best practices. The OCIO has initiated this project without a complete understanding of the scope of OPM's existing technical infrastructure or the scale and costs of the effort required to migrate it to the new environment.

In addition, we have concerns with the nontraditional Government procurement vehicle that was used to secure a sole-source contract with a vendor to manage the infrastructure overhaul. While we agree that the sole-source contract may have been appropriate for the initial phases of securing the existing technical environment, we do not agree that it is appropriate to use this vehicle for the long-term system migration efforts.

We intend to conduct further oversight of this Project and may issue additional reports in the future. However, we have identified substantial issues requiring immediate action, and we are therefore issuing the following recommendations in this Flash Audit Alert, so that the OCIO can immediately begin taking steps to address these concerns. We provided a draft of this Alert to the OCIO for their review, but we did not receive any comments.

[1] This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (http://www.opm.gov/our-inspector-general), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

1) **Project Management Activities**

We were told that OPM officials initiated the Project to improve the security of its network and operating environment after learning of a significant security incident in March 2014. The initial plan was to make major security improvements to the existing environment and continue to operate OPM systems in their current location. During the process of implementing security upgrades, OPM determined that it would be more effective to completely overhaul the agency's IT infrastructure and architecture and move it into a completely new environment.

The new plan involves hosting OPM systems in two commercial data centers. The new architecture will be a distributed computing environment, with no mainframe or legacy applications. We have been told by OCIO officials that no applications will be allowed to migrate to the new Shell environment unless they are rebuilt to be compatible with all new security and operating features of the new architecture. The phases of this Project include Tactical (shoring up the existing security environment), Shell (creating the new data center and IT architecture), Migration (migrating all OPM systems to the new architecture), and Cleanup (decommissioning existing hardware and systems). The current status is that the Tactical phase is complete, and the Shell phase is underway.

While we agree in principle that this is an ideal future goal for the agency's IT environment, we have serious concerns regarding OPM's management of this Project. The Project is already underway and the agency has committed substantial funding, but it has not yet addressed several critical project management requirements, including, but not limited to:

- OPM has not yet identified the full scope and cost of this project;
- OPM has not prepared a 'Major IT Business Case' (formerly known as the OMB Exhibit 300), as required by OMB for IT projects of this size and scope; and,
- OPM's overall project management process is missing a number of critical artifacts considered to be best practices by relevant organizations.

As a result, there is a high risk that this Project will fail to meet the objectives of providing a secure operating environment for OPM systems and applications.

Many critical OPM applications (including those that process annuity payments for Federal retirees, reimburse health insurance companies for claims payments, and manage background investigations) run on OPM's mainframe computers. These applications are based on legacy technology, and will need to be completely renovated to be compatible with OPM's proposed new IT architecture.

To help put this in perspective, we reference OPM's Fiscal Year (FY) 2009 efforts to migrate a single financial system application from the mainframe. This project was relatively well managed and was subject to oversight from several independent entities, including the OIG, but it still required two years and over $30 million to complete. OPM's current initiative is much more massive than this prior project, as each individual application migration should

be treated as its own project similar to this example. Furthermore, there are many other systems besides OPM's mainframe applications that will also need to be modified to some extent to be compatible.

The Migration phase of this Project will clearly be a complex, expensive, and lengthy process. OPM currently estimates that it will take 18 to 24 months to complete. We believe this is overly optimistic and that the agency is highly unlikely to meet this target. In fact, OPM is still in the process of evaluating its existing IT architecture, including the identification of all mainframe applications that will need to be migrated, and other systems that will need to be redesigned. OCIO representatives are currently conducting a compatibility assessment for the "major OPM investments" as encompassed by three program offices: Retirement Services, Federal Investigative Services, and Human Resources Solutions. It was explained to us that this review only addresses approximately 80 percent of OPM's systems, with the remainder considered out of scope for this evaluation, but to be eventually addressed. This assessment is not scheduled for completion until next month (July 2015). It is difficult to see how the agency can estimate its timeline when it does not yet know the scope of the effort.

Related to the unknown scope of the Project is the uncertainty of its overall cost. OPM has estimated that the Tactical and Shell phases of the Project will cost approximately $93 million. OMB has included $21 million in the President's FY 2016 budget to fund part of this amount. Another $5 million was contributed by the Department of Homeland Security to support its continuous monitoring program, and the remaining $67 million is being collected from OPM's major program offices as a special assessment. However, this estimate does not include the costs to migrate the many existing applications to the new IT environment, which are likely to be substantial.

When we asked about the funding for the Migration phase, we were told, in essence, that OPM would find the money somehow, and that program offices would be required to fund the migration of applications that they own from their existing budgets. However, program office budgets are intended to fund OPM's core operations, not subsidize a major IT infrastructure project. It is unlikely that OPM will be able to fund the substantial migration costs related to this Project without a significantly adverse impact on its mission, unless it seeks dedicated funding through Congressional appropriation. Also, OPM's current budget approach seems to violate IT spending transparency principles promoted by OMB's budget guidance and its IT Dashboard initiative, which is intended to "shine [a] light onto the performance and spending of IT investments across the Federal Government."

In addition to the undefined scope and uncertain budget, OPM has not completed other standard, and critical, project management steps. Control Objectives for Information and Related Technology (COBIT) is a framework created by the Information System Audit and Control Association (ISACA) for IT management and IT governance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework also identifies internal controls required for effective organizational management.

COBIT and the COSO framework define best practices for major IT developments. Several examples of critical processes that OPM has not completed for this project include:

- Project charter;
- Comprehensive list of project stakeholders;
- Feasibility study to address scope and timeline in concert with budgetary justification/cost estimates;
- Impact assessment for existing systems and stakeholders;
- Quality assurance plan and procedures for contractor oversight;
- Technological infrastructure acquisition plan;
- High-level test plan; and,
- Implementation plan to include resource planning, readiness assessment plan, success factors, conversion plan, and back-out plan.

In our opinion, the project management approach for this major infrastructure overhaul is entirely inadequate, and introduces a very high risk of project failure. The correct approach would be to use the OMB budget process to request project funding using the OMB-required Major IT Business Case (Exhibit 300) process. This would require OPM to fully evaluate the costs, benefits, and risks associated with its planned Project, and present its business case to OMB to seek approval and funding.

OMB Circular A-11 Appendix 6 defines capital budgeting requirements for capital asset projects. The basic concepts are that capital asset projects require proper planning, cost/benefit analysis, financing, and risk management. This includes demonstrating that the return on investment exceeds the cost of funds used, and an analysis of the "investment's total life-cycle costs and benefits, including the total budget authority required for the asset..."

Furthermore, the financing principles outlined in the Circular state that "Good budgeting requires that appropriations for the full cost of asset acquisition be enacted in advance to help ensure that all costs and benefits are fully taken into account at the time decisions are made to provide resources."

Finally, the Circular requires risk management and earned value management throughout the life-cycle of the project: "The investment cost, schedule, and performance goals established through the Planning Phase of the investment are the basis for approval to procure the asset and the basis for assessing risk. During the Procurement Phase, performance-based management systems (earned value management system) must be used to provide contractor and Government management visibility on the achievement of, or deviation from, goals until the asset is accepted and operational."

OMB's FY 2016 IT Budget – Capital Planning Guidance further states that "Together, the Major IT Business Cases and Major IT Business Case Details provide the budgetary and management information necessary for sound planning, management, and governance of IT investments. These documents help agencies explicitly align IT investments with strategic and performance goals, and ultimately provide value to the public by making investment and

management information more transparent." OMB expects that artifacts, documents, and associated data similar to those defined by the COBIT and COSO frameworks already exist when a Major IT Business Case is submitted as part of an agency's budget process.

OPM officials informed us that the urgent and compelling nature of the situation required immediate action, and this is the reason that some of the required project management activities were not completed. We agree with and support the agency's efforts to improve its IT security infrastructure through the Tactical phase of this Project. We understand and accept that immediate action was required and that it was appropriate to do so. However, the other phases of the project are clearly going to require long-term effort, and, to be successful, will require the disciplined processes associated with proper system development project management.

Without these disciplined processes, there is a high risk that this Project will fail to meet all of its stated objectives. In addition, without a guaranteed source of funding in place, OPM may not have the internal resources necessary to complete the Migration phase, which is likely to be complex and expensive. In this scenario, the agency would be forced to indefinitely support multiple data centers, further stretching already inadequate resources, possibly making both environments less secure, and increasing costs to taxpayers. This outcome would be contrary to the stated goals of creating a more secure IT environment at a lower cost.

Recommendation 1

We recommend that OPM's OCIO complete an OMB Major IT Business Case document as part of the FY 2017 budget process and submit this document to OMB for approval. Associated with this effort, the OCIO should complete its assessment of the scope of the migration process, the level of effort required to complete it, and its estimated costs. Furthermore, the OCIO should implement the project management processes required by OMB and recommended by ISACA's COBIT and the COSO framework.

2) **Sole-Source Contract**

OPM has secured a sole-source contract with a vendor to manage the infrastructure improvement project from start to finish. Although OPM completed a Justification for Other Than Full and Open Competition (JOFOC) to justify this contract, we do not agree that it is appropriate to use this contract for the entire Project.

The initial phase of the Project covered the procurement, installation, and configuration of a variety of software tools designed to improve the IT security posture of the agency (the Tactical phase). We agree that recent security breaches at OPM warranted a thorough and immediate reaction to secure the existing environment, and that the JOFOC was appropriate for this tactical activity.

However, the JOFOC also covered subsequent phases of the Project related to the development of the new Shell infrastructure, the migration of all of OPM's applications into

this new environment, and decommissioning the old environment. Although the Shell phase is largely complete, there is still an opportunity to procure contractor support for the migration and cleanup phases of this project using the appropriate contracting vehicles. Without submitting this Project to an open competition, OPM has no benchmark to evaluate whether the costs charged by the sole-source vendor are reasonable and appropriate.

As stated previously, we expect the Migration phase to be extremely complex and time consuming. It will likely require significant contractor support, with each application requiring a unique skill set. OPM may also determine that it would benefit from a contractor to oversee the Migration effort as a whole. We believe that contractor support for both application-specific migration and the Migration and Cleanup efforts as a whole are not justifiably covered by the existing sole-source contract. FAR 6.302 outlines seven scenarios where contracting without full and open competition may be appropriate, two of which relate to an unusual and compelling urgency and national security implications. However, we have not been provided evidence that the Migration and Cleanup phases of this project meet the FAR criteria for bypassing an open competition.

We believe that OPM should gain a complete and thorough understanding of the scope of this Project, request funding from OMB via the appropriate avenues (See Recommendation 1) and *then* subject the remainder of the project to contracting vehicles other than the sole source contract used for the Tactical and Shell phases.

Recommendation 2

We recommend that OPM not leverage its existing sole source contract for the Migration and Cleanup phases of the infrastructure improvement project. Contractor support for these phases should be procured using existing contracts already supporting legacy information systems or via full and open competition.

If you have any questions about this Flash Audit Alert you can contact me, at 606-1200, or your staff may wish to contact Michael R. Esser, Assistant Inspector General for Audits, at 606-2143.

cc: Chris Canning
Acting Chief of Staff

Angela Bailey
Chief Operating Officer

Janet Barnes
Director, Internal Oversight and Compliance

Donna K. Seymour
Chief Information Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

June 22, 2015

MEMORANDUM FOR PATRICK E. McFARLAND
Inspector General

FROM: KATHERINE ARCHULETA
Director

SUBJECT: Response to Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055)

Thank you for your diligence in issuing the Flash Audit Alert referenced above. The U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project represents an aggressive effort by the agency to modernize IT infrastructure and further strengthen security capabilities. I very much appreciate your support of this project, particularly in light of recent events, and look forward to continuing to work with your office to ensure that it is executed efficiently, effectively and in compliance with applicable law, guidance and best practices as appropriate.

Upon completion of a detailed review of the Flash Audit Alert, OPM has identified and outlined below areas of agreement and disagreement. I appreciate your consideration of this response, and would welcome the opportunity to discuss it further at your convenience.

Recommendation 1 states that OPM's Office of the Chief Information Officer (OCIO) should complete its assessment of the scope of the Migration process. OPM agrees with this recommendation and is planning to complete this process within the next several months. It is also recommended that the level of effort to complete the Migration process and the estimated costs of the Migration process should be assessed. OPM agrees with this as well, which is why these two evaluations are an ongoing part of not just the Migration process, but in all phases of the information technology protocol assessment. These evaluations may require our estimated costs to change as developments demand. Should that be the case, however, OPM will continue to update, track, document, and justify those changes.

It is further recommended that the OCIO "should implement the project management processes required by OMB." OPM agrees, and this is why we have been engaged in such implementation. OPM does not agree, however, with the recommendation that OPM should follow the project management processes recommended by ISACA's COBIT and COSO framework. OPM adheres to the OPM Systems Development Life Cycle, derived from Federal standards to manage OCIO Portfolios, Programs and Projects, rather than commercial industry frameworks.

Recommendation 1 advocates that the OCIO "complete an OMB Major IT Business Case document" and that this effort be taken as part of the FY 2017 budget process to be submitted to OMB for their approval. However, reports for an OMB Major IT Business Case document must be written so that they are ready for submission by early August. Completing and submitting an initial OMB Major IT Business Case document requires anywhere from eight months to a year of research, consultations, discussion, and effort. In order to submit such a request for the FY 2017 budget process, it would be necessary for OPM to begin a process that could not be completed in time and that would only serve to stall the critical efforts already underway. Further, Recommendation 1 fails to acknowledge that in July of 2015, OPM is not seeking to adjust our business case for our FY 2016 numbers since the Shell phase of the infrastructure improvement process will be mostly completed by the end of FY 2015. Further, in our FY 2016 Congressional Budget Justification, OPM did request $21 million to "implement and sustain agency network upgrades" which were first initiated in FY 2014, as well as for "security software maintenance to ensure a stronger, more reliable, and better protected OPM network architecture."

Recommendation 1 would not only require OPM to put aside efforts already underway to address OPM's information technology needs, but it also ignores how OPM has made its budget requests in connection with the infrastructure improvement project. For instance, the Tactical solutions, developed in response to the March 2014 breach, were extensions of the existing network, and all procurements were made in consultation with OMB and other stakeholders due to exigent circumstances. Following implementation of the Tactical solutions, it became apparent that OPM would need to move to the next stage, which is now referred to as Shell. However, the Shell was not designed until September 2014, after the Major IT Business Case submission cycle for FY 2014. If the Shell had to wait until a Major IT Business Case was made during the FY 2015 cycle, a year would have passed. Instead, OPM was able to justify its efforts related to the Shell by tying this effort to earlier funding requests, which allowed for more expeditious approval. The Shell will be complete by August 2015 and made available by September 2015. A similar scenario exists going forward – the Migration activities will be specific to the systems affected and are therefore extensions of the investments tracked by the owners of these systems. As such, the Migration activities are connected to the justifications put forward by the owners of these systems. OPM understands and respects that the goal of a Major IT Business Case document is to justify funding given to a program and to track how funds are spent. OPM, however, is not operating outside of documentation, justification, and tracking requirements just because we are not generating a new Major IT Business Case document for FY 2017. We are working with OMB to document all of our expenditures and linking our needs in order to provide quick responses to existing justifications and efforts.

OPM agrees with the majority of your Recommendation 2. In this recommendation, you state that OPM should "not leverage its existing sole source contract for the Migration and Cleanup phases of the infrastructure improvement process" that OPM is undertaking. OPM agrees and would like to take this opportunity to point out that the contract for the Migration and Cleanup phases of the infrastructure improvement project have not yet been awarded.

However, you state, "While we agree that the sole-source contract may have been appropriate for the initial phases of securing the existing technical environment, we do not agree that it is appropriate to use this vehicle for the long-term system migration efforts." The underlying

assumption in this statement – that a sole-source contract is in place for the Tactical, Shell, Migration, and Cleanup phases of the infrastructure improvement process – is incorrect.

This misperception is compounded in another point in your memorandum when you state that "OPM has secured a sole-source contract with a vendor to manage the infrastructure improvement project from start to finish." The memorandum also states that "However, the JOFOC also covered subsequent phases of the Project related to the development of the new Shell infrastructure, the migration of all of OPM's applications into this new environment, and decommissioning the old environment." Both of these statements represent a misunderstanding of the procurement plan and we would welcome an opportunity to clarify this further.

Recommendation 2 also advocates that "contractor support for these phases should be procured using existing contracts already supporting legacy information systems or via full and open competition." OPM agrees, as this recommendation is consistent with law governing Federal contracting and procurement requirements and with Office of Management and Budget (OMB) guidance. OPM plans to conduct its contracting on the Mitigation and Cleanup phases of the infrastructure improvement process in a way that is consistent with these authorities.

You note that "Although the Shell phase is largely complete, there is still an opportunity to procure contractor support for the migration and cleanup phases of this project using the appropriate contracting vehicles." Please bear in mind that unless the awarding of the contract would be reasonable and appropriate, OPM is prohibited from awarding the contract. In completing the analysis on what is the most reasonable and appropriate course of action, OPM will submit to its available contract avenues and determine the best possible business decision.

There are discussions within the surrounding materials in your memorandum with which OPM either disagrees, sees the potential to disagree, or does not understand. For example, the memorandum expresses concern that OCIO has not followed OMB requirements and project management best practices. OPM disagrees, as we have been in continual consultation and discussion with OMB and other stakeholders on this effort. The memorandum expresses concern that the size, scope, and cost of the undertaking are not completely understood by the OCIO. OPM and the OCIO have always been very clear that the undertaking includes factors and costs that will be understood more clearly as the Project proceeds.

Further, you state in the first page of the memorandum that OPM is following a "nontraditional Government procurement vehicle." Regardless of its traditional or nontraditional nature, the procurement process followed by the Department of Homeland Security (who serves as the contracting office) is compliant with applicable law.

In expressing your views in the use of contractors with unique skill sets to support OPM's efforts with which, again, OPM generally agrees – you suggest that OPM may "determine it would benefit from a contractor to oversee the Migration effort as a whole." While OPM may ultimately rely on a contractor for this function, this appears to be a responsibility that would be best handled by the OCIO. It's important that these efforts be centralized in a common source who has the best interests of the American taxpayer in mind. OPM suggests it would be more

efficient and cheaper to maintain this function with the Federal government and not to place this responsibility in the hands of a contractor.

Finally, you state that OPM's OCIO did not provide comments in reaction to your draft memorandum. While it is true that OPM's OCIO did not provide written comments prior to issuance of the Audit, it is important to point out, however, that numerous representatives from your office met with the OCIO on May 26, 2015, during which verbal comments similar to those provided above were conveyed. Unfortunately, the written comment period you established coincided with the timing of several critical developments related to the recent cybersecurity incidents. OPM OCIO's attention and resources were, understandably, focused on responding to those developments and we were unable to provide comments in the requested timeframe. However, I appreciate your consideration of the responses outlined in this memorandum and look forward to continued collaboration between our offices on this critical project.

The Wall Street Journal

Altegrity Executives Got Payouts Before Security Screener Filed for Bankruptcy

Payments of $26 million at company whose US Investigations Services unit vetted Snowden and Navy Yard gunman

By Peg Brickley
Updated April 24, 2015 8:54 p.m. ET

Newly released court records show that Altegrity Inc., a company linked to some notable U.S. security stumbles of recent years, shelled out $25.7 million to top executives the year before it filed for bankruptcy protection.

Some of the money was channeled through Altegrity subsidiary US Investigations Services, which vetted Edward Snowden for his National Security Agency contract work. The company also conducted the background check on Aaron Alexis, an employee of a government subcontractor who killed 12 people in a shooting rampage at the Washington Navy Yard in September 2013.

Altegrity, which is based in Falls Church, Va., has denied doing shoddy work. It filed for bankruptcy protection in February after losing the federal contracts that accounted for over one-third of its revenue. On Thursday, the company said executive bonuses handed out as it headed to bankruptcy were part of agreements put in place in 2013 and 2014 as it cut costs and streamlined the organization.

The payments to 29 top-ranking executives of Altegrity and its subsidiaries included $3.6 million to leaders of US Investigations, or USIS, the unit whose failings made headlines and triggered the bankruptcy filing.

US Investigations Services, a unity of Altegrity, vetted Edward Snowden for work at the National Security Agency. Mr. Snowden later leaked sensitive information on U.S. electronic surveillance. PHOTO: THE GUARDIAN/REUTERS

USIS lost its contracts to do background checks for the federal government last year after suffering a cyberattack that exposed the files of 25,000 Department of Homeland Security employees to hackers. The company has denied wrongdoing in connection with the cyberattack.

The cyberattack was the just latest blow to USIS after the Navy Yard shootings and Mr. Snowden's leaks of sensitive information, which surfaced in newspapers in June 2013. Allegations of bad practices at the company first surfaced in a 2011 whistleblower lawsuit that accused USIS of denoting some incomplete investigations as being concluded and ready for payment. Later joined by the U.S. Department of Justice, the case sought to recoup payments USIS collected for allegedly faulty background checks of applicants for posts requiring federal security clearance.

Altegrity said the background checks on Mr. Snowden and Mr. Alexis were not at issue in the whistleblower case, and that the company was cooperating with the Justice Department. Altegrity's bankruptcy filing stalled action in the lawsuit, which is now before a federal judge in Washington, D.C.

Until its contracts were cut off, USIS did work for the Department of Homeland Security, the Justice Department, the Social Security Administration, the U.S. Office of Personnel Management, the U.S. Postal Service and the U.S. Capitol Police, court papers say.

Last year's loss of the federal government contracts cut deeply into revenue for Altegrity, which had been raking in hundreds of millions of taxpayer dollars annually. USIS accounted for 39% of Altegrity's total net revenue for the 12 months through June 30, 2014, but its contribution waned with the end of the government contracts and thousands of people lost their jobs. The company had gross revenue of about $245 million for its fiscal year ended September 2014.

Those at the top of the troubled unit, however, collected extra compensation. Now-departed Chief Executive Sterling Phillips, who had fielded questions from lawmakers critical of USIS's performance, collected $1 million in bonuses and severance pay months after the contracts were lost, when the company had begun shutting down. Mr. Phillips joined the company in 2013 as part of a new leadership team summoned in the wake of the whistleblower suit.

"Many of the performance-based payments were made in connection with agreements put in place in 2013 and early 2014 related to the restructuring of Altegrity that occurred at that time to reduce costs and streamline the organization. The amount, timing and criteria for the payments were part of the agreements, and the agreements themselves were based on standard practices and benchmarks," Altegrity said Thursday.

Altegrity agreed to release the numbers after Dow Jones & Co., which publishes The Wall Street Journal, objected to the company's motion to keep its insider pay information under wraps during bankruptcy proceedings.

Some of the extra prebankruptcy payments to executives noted in filings in U.S. Bankruptcy Court in Wilmington, Del., were linked to the sale of businesses, according to Altegrity, or went to executives of "business units that were performing well."

While USIS is being dissolved, Altegrity's Kroll and HireRight businesses, which provide security and employment screening services mostly for private companies, are being preserved as part of the bankruptcy turnaround.

USIS paid $125,000 to the former chairman of the Joint Chiefs of Staff, retired Adm. Michael G. Mullen, who was called on for advice around the time the unit's government contracts began to slip away. Mr. Mullen is identified as an insider because he is a senior adviser to Providence Equity Partners, the Rhode Island buyout firm that owns USIS and Altegrity.

Providence, led by Jonathan M. Nelson, bought USIS for about $1.5 billion from the Carlyle Group CG -0.06 % in 2007. A year later, USIS combined with HireRight, and in 2010 Providence, which manages some $40 billion in assets, acquired Kroll from Marsh & McLennan Cos. for $1.1 billion.

At the outset of bankruptcy proceedings, Altegrity disclosed what it paid its leaders only to creditors pledged to secrecy, including the official committee representing unsecured creditors and to federal bankruptcy watchdogs. The company maintained it should be excused from bankruptcy disclosure rules because it operates "in highly competitive markets where the acquisition and retention of talent is critical to success."

BUSINESS INSIDER

Hedge fund manager who said 'sorry' for losing 99.7% of his clients' money is now being investigated by the SEC and DOJ

JULIA LA ROCHE
MAR. 27, 2015, 3:31 PM

The Department of Justice and the Securities and Exchange Commission are investigating how the 28-year-old manager of Canarsie Capital lost nearly all of the $60 million hedge fund's capital in just three weeks of trading, according to a letter sent to the fund's investors.

The February 12th letter informing the fund's investors about the governmental investigation was sent by Ken deRegt, one of the hedge fund's partners, via his attorney from Skadden Arps.

A spokeswoman for the SEC declined to comment. The DOJ said it could neither confirm nor deny whether a matter is under investigation. Benjamin Kaplan, the attorney for the fund's 28-year-old founder Owen Li, also declined to comment.

Flickr/ kenfieura with photoshop by Business Insider

Canarsie Capital was named after the neighborhood in Brooklyn where Owen Li grew up.

"I am very sorry"

On January 20, Owen Li, the principal of New York-based Canarsie Capital, wrote an apology letter to investors stating that he "engaged in a series of aggressive transactions" during the first three weeks of 2015 that resulted in him losing all but $200,000 of the fund's capital.

In other words, he lost 99.7% of the firm's money.

"Words cannot express how sorry I feel for causing this loss to you, and to the entire Fund," he said. "I am very sorry for causing this result, and for failing you and the Fund. No doubt you will be angry about this--and I am truly sorry."

declined to comment.

SS&C Technologies, one of the largest and most reputable hedge fund administrators, served as Canarsie's administrator and provided the reports to investors. SS&C didn't respond to requests for comment.

The SEC and DOJ investigation

In mid-February, Canarsie's investors received a letter from Ken deRegt via his attorney at Skadden, Arps. His attorney didn't respond to multiple requests for comment and the letter is the last communication investors have received from the fund.

The letter, dated Feb. 12, explained that Li had been "unwilling" to step aside as he had previously told investors in another communication that he would do.

DeRegt's letter also said that the DOJ and SEC have opened investigations into the events at Canarsie.

Initially, deRegt and some of the fund's investors had hired an independent firm to conduct a review of what happened at Canarsie. That private investigation, though, has been suspended while the governmental one is ongoing, the letter indicates.

Was Li lying about his P&L?

The Feb. 12 letter suggests that Li may have been lying about his P&L statements (profits and losses) in daily internal trading reports.

According to letter, Goldman's records showed that the fund had $58 million at the end of December 2014 and SS&C's records showed about $56 million for that same period. Those records, which deRegt writes weren't available to him before, also showed that fund had suffered about a 10% loss in December. According to deRegt's letter, the daily reports he had received from Li during that indicated a 5% loss.

What's more, deRegt writes that daily internal reports he received from Li showed "modest additional losses and substantially reduced risk." The reports deRegt received from Li did not reflect the trading activity in Goldman's records.

"For example on Jan. 16 the daily internal reports indicated a portfolio valuation of approximately $60 million. In fact the assets on deposit with Goldman on that date were only $220,000."

What next?

Canarsie Capital failing isn't really systemically significant. Relatively speaking, the fund was small. It was also a start-up and failures do happen in this space.

However questions remain about whether or not Li was acting illegally, and how he was able to continue trading as funds disappeared from Canarsie's brokerage account.

For now, we'll have to wait for the results of the governmental investigation.

If you have any additional information regarding the events at Canarsie Capital, feel free to

Questions for The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management

Questions from Chairman Jason Chaffetz
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

---

1. As Chairman Chaffetz requested at the June 24 hearing, please provide a copy of OPM's response to Senator Warner's June 19 letter to OPM regarding the contract to Winvale/CSID.

We refer the Committee to Senator Warner.

2. At the June 24 hearing, CIO Donna Seymour was asked why OPM did not use existing GSA contract vendors for identity theft services. Generally, she said that the GSA vendors did not offer all the services that OPM wanted to provide. As an example of such services, she said the GSA vendors did not offer de-duplication services. Please describe in full the services that OPM wanted to provide that were not available through the GSA vendors.

OPM sought to put in place a contract that would provide services over a number of years and would allow for notifications and services for any future cyber incidents. In addition to the de-duplication services, OPM sought a vendor that had the ability to look at single bureau credit monitoring and reporting, and provide individual unit prices for the services provided.

3. How many other companies submitted proposals for the contract besides Winvale/CSID? Please identify these other contractors who submitted proposals.

The information requested by Congress is considered to be bid or proposal information/source selection information. The recipient of this response is notified (pursuant to the requirements of the Federal Acquisition Regulations (FAR) Part 3.104), that the disclosure of the information provided is restricted by 41 U.S.C. chapter 21.

OPM received a total of three quotation responses as a result of the open market solicitation. Those quotation responses received and evaluated by OPM were from Winvale, ID Experts, and Experian.

4. Has OPM made a decision about whether to extend the services provided by Winvale/CSID beyond the initial 18 months? If so, please provide an estimate of costs.

If an individual was affected by the incident involving personnel data, he or she has been sent a notice that includes information about the free services available for 18 months. As part of this service, individuals are *automatically* enrolled in:

- **Full service identity restoration, which helps to repair your identity following fraudulent activity;**
- **Identity theft insurance, which can help to reimburse you for certain expenses incurred if your identity is stolen.**

Instructions on how to enroll in other services were included in the notification.

In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

5. Does OPM plan to exercise the option periods of the Winvale/CSID contract? Please explain.

There are no options to exercise with this contract. Services will be provided for 18 months.

6. Does OPM maintain service credit records, retirement records, or any personnel records for current or former agents with the Central Intelligence Agency (CIA)? If so, please explain which specific records are maintained by OPM and whether such records were compromised during the recent incidents? If not, please explain why current and former CIA agents received notifications from OPM that their infomation may have been compromised?

OPM is working closely with DOD and the Intelligence Community on the appropriate notifications for individuals in sensitive positions.

Questions for The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management

Questions from Representative Michael R. Turner
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

1. As you may know, my Congressional district is home to Wright-Patterson Air Force Base, the largest single-site employer in the State of Ohio. I am concerned that OPM's response to the data breaches does not seek to adequately protect Wright-Patterson Air Force Base personnel whose the personal information may have been compromised as a result of these breaches. Please provide me with the specific steps you are taking to assist these individuals and their families.

We have sent notifications to those affected by the incident involving personnel data. We are offering free identity theft monitoring and restoration services. If an individual was affected by this incident, they have been sent a notice that includes information about the free services available to them for 18 months. As part of this service, they are *automatically* enrolled in:

- **Full service identity restoration, which helps to repair their identity following fraudulent activity; and**
- **Identity theft insurance, which can help to reimburse them for certain expenses incurred if their identity is stolen.**

In addition, we are providing information on our website to educate individuals on ways to protect their identity.

For those affected by the background investigation incident, an online resource, www.opm.gov/cybersecurity, has been created. The site offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.

Impacted individuals will receive a notice in the mail providing details on the incident and the services available to them at no cost for at least three years such as:

- **Full service identity restoration support and victim recovery assistance**
- **Identity theft insurance**
- **Identity monitoring for minor children**
- **Continuous credit monitoring**
- **Fraud monitoring services beyond credit files**

In the coming weeks a call center will be opened to respond to questions and provide more information. If an individual is affected, he or she will not be able to receive personalized

information until notifications begin, and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that have questions, and OPM will work with its partners to establish this call center as quickly as possible.

In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

2. Why is the identity theft insurance coverage limited to eighteen months? What processes or analysis led you to conclude that eighteen months was sufficient to protect these individuals?

OPM is offering free identity theft monitoring and restoration services to those affected by the incident involving personnel data. If an individual was affected by this incident, they have been sent a notice that includes information about the free services available to them for 18 months. As part of this service, they are *automatically* enrolled in:

- **Full service identity restoration, which helps to repair their identity following fraudulent activity; and**
- **Identity theft insurance, which can help to reimburse them for certain expenses incurred if their identity is stolen.**

Identity Theft Insurance covers costs associated with identity restoration for up to $1 million. There is no deductible.

A careful and thoughtful analysis of the risk presented by the personnel records incident as well as a review of the services available, precedent, and industry best practices led OPM to conclude that 18 months was the appropriate duration for the comprehensive suite of services offered to help federal employees in the personnel files incident.

3. The information required to be included in the background check Standard Form 86 (SF-86) is extensive. What steps are you taking to assist individuals (relatives, references, etc.) whose information was submitted as part of an SF-86 submission?

There are a number of resources available to assist individuals who information was submitted as part of the SF-86.

- **Currently the following services are being provided to impacted individuals from the personnel records incident:**
  - **Automatic enrollment in identity restoration and theft insurance;**
  - **An online cybersecurity resource center at https://www.opm.gov/cybersecurity which offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional**

frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.

- **A Congressional hotline, for Members and staff, to assist with questions for their constituents.**
- **An automated phone message providing further information for the federal workforce and the public.**
- **A call center in the coming weeks to respond to questions and provide more information.**

- **Once a notification contract is awarded, and notifications begin to be sent out to impacted individuals, the following additional resources will be available:**
  - **Every individual whose Social Security Number was stolen will receive a notification letter. This letter will be accompanied by an information brochure with information that should be shared with relatives or references who may have been listed on an individual's SF-86 form.**
  - **A comprehensive suite of monitoring and protection services – such as identity restoration support, identity theft insurance, identity monitoring for children, continuous credit monitoring, and additional fraud monitoring services – for at least three years to the applicants and non-applicants with Social Security Numbers and other sensitive information that was stolen.**

This approach builds upon the lessons learned from prior cybersecurity incidents, and ensures that those affected and the public at-large have the information and resources they need to guard against cyber threats. OPM is working as quickly as possible with GSA and DOD on a new contract to notify and provide services for the individuals affected by the background investigation records incident. As part of this process, OPM has benefited from and would like to continue conversations with stakeholders such as Federal employee unions, to hear their feedback and concerns regarding the notification process for the personnel records incident.

Questions for The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management

Questions from Representative Tim Walberg
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

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?

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

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

OPM is moving to a Zero Trust tenet posture. All new architecture use this approach and existing systems are being migrated. These legacy systems were not built to perform at a Zero Trust tenet posture; therefore the migration process will be slower than the build out of new architecture.

OPM continues to explore all opportunities provided by commercial industry leaders. OPM made a decision in mid-2014 that numerous OPM systems would need to be protected at the highest levels. OPM is vigorously pursuing implementation of its target environment. The cyber sprint has significantly influenced OPM, as OPM has significantly influenced the cyber sprints. It is important to note that OPM is in the top quartile of agencies that accelerated use of multi-factor authentication for both privileged and non-privileged users. . OPM is confident in its plan, developed in 2014, but will remain nimble to accommodate advancements in technology or additional needs. We remain committed to a more secure environment.

Questions for The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management

Questions from Representative Steve Russell
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

1. What data specifically was breached pertaining to SF-86 files? Was it just the form specifically, or full background investigation notes?

Social Security numbers (SSNs) and other sensitive personally identifiable information (PII) was stolen for anyone who underwent a background investigation by submitting an SF-86, SF-85P or SF-85 form, and non-applicants such as spouses and co-habitants whose SSN and other sensitive PII were provided by the applicant. Identifying information in these records about applicants include details such as SSNs, residency and educational history, employment history and activities, information about immediate family and other personal and business acquaintances, health, criminal and financial history, and other details. Also, information recorded during the investigation process was stolen for some applicants. Beyond the information on an individual's SF-86 or 85, some background investigation records also include findings from interviews conducted by background investigators and include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. While background investigation records do contain some information regarding mental health and financial history provided by those that have applied for a security clearance and sources contacted during the background investigation, there is no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of Federal personnel were impacted by this incident (i.e. annuity rolls, retirement records, USA JOBS, Employee Express).

2. What steps has OPM taken to protect the identity and credit of family members, including spouses, dependents, and cohabitants whose information was breached by the loss of SF-86 data? Will OPM extend the same identity theft protections to those individual as they have to federal employees?

OPM is taking the following steps to assist Federal employees and other individuals:

1. **Providing a comprehensive suite of monitoring and protection services – such as identity restoration support, identity theft insurance, identity monitoring for children, continuous credit monitoring, and additional fraud monitoring services – for at least three years to the to any individuals whose Social Security Numbers was stolen during this cyber incident. In most cases, minor children's social security number was not included on the SF-86 form; however due to the**

risk associated with identify theft of minors, all impacted applicants will have the option of signing up a current minor children whose information was listed on the background investigation form for identity theft monitoring services.

2. **Every individual whose Social Security Number was stolen will receive a notification letter. This letter will be accompanied by an information brochure with information that should be shared with relatives or references who may have been listed on an individual's SF-86 form.**
3. **Establishing an online cybersecurity resource center at https://www.opm.gov/cybersecurity which offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.**
4. **Establishing a call center in the coming weeks to respond to questions and provide more information. In the interim individuals are encouraged to visit https://www.opm.gov/cybersecurity.**
5. **Explore a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future.**

This approach builds upon the lessons learned from prior cybersecurity incidents, and ensures that those affected and the public at-large have the information and resources they need to guard against cyber threats. OPM is in the contracting process for a Vendor and will be sharing information regarding the contracting process at a later date.

Questions for The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management

Questions from Representative Brenda Lawrence
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

1. OPM relies on contractors to handle the government's background investigations. USIS used to be the largest private contractor performing this function, and KeyPoint is now the largest.

   a. What steps has OPM taken since the USIS and KeyPoint data breaches to ensure that contractors are doing a better job with cyber security?

In alignment with recommendations made by the GAO, OPM is in the process of developing, documenting, and implementing enhanced oversight procedures for ensuring that a system test is fully executed for each contractor-operated system. These procedures will expand the policy for oversight of contractor systems currently in OPM's IT Security and Privacy Handbook. In alignment with another recommendation of the IG, as OPM considers the appropriate avenues for the Mitigation and Cleanup phases of the infrastructure improvement process, it will conduct a thorough analysis on the most reasonable and appropriate course of action, and explore all available contracting avenues to determine the best option for the health of its modernization project and for the taxpayer.

Additionally, Inspector General Patrick McFarland is conducting a series of audits around this issue. IG McFarland and Acting Director Cobert are meeting regularly to discuss the issues that the IG has raised.

   b. Is OPM requiring additional or more specific cyber security measures for its contractors? If so, what are they, and how are these new requirements being implemented?

OPM is working with Keypoint on the following:

- **Audit and inspection by third party authentication organizations**
- **OPM OIG audit and inspection**
- **Policy and process changes that have eliminated the retention of unnecessary data**
- **The full implementation of two factor PIV authentication with OPM**
- **Continued unfettered assistance in the deployment of additional OPM security requirements**

   c. How is OPM monitoring the compliance of contractors with those new requirements?

OPM will establish requirements for future contracts, as appropriate, to ensure access to contractor systems in the event of an incident. This will ensure that OPM and law enforcement agencies can access data and conduct effective and immediate response in

the case of any future cyber incidents. OPM will also consider whether any additional authorities from Congress are needed in order to enforce such access.

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL

Response to Questions for the Record
Submitted by Representative Tammy Duckworth
Committee on Oversight and Government Reform
Hearing on "OPM Data Breach: Part II"
June 24, 2015

1. The cyber-attacks on USIS and KeyPoint, which resulted in the compromising of tens of thousands of sensitive government personnel records, highlight the serious risks of third-party vendor security at federal agencies. I understand that your office conducted an audit in 2014 of OPM's information technology security programs.

    a. In conducting your audit, did you examine whether OPM had any vulnerabilities with respect to third-party vendor security? If so, what were the vulnerabilities that you found?

        ***OPM OIG Response**: In Fiscal Year (FY) 2014 OPM's major system inventory contained 22 systems operated by a contractor. In completing the FY 2014 FISMA metrics provided by the U.S. Department of Homeland Security, we evaluated whether all OPM systems, including these contractor systems, had met FISMA requirements related to contingency planning, security controls testing, and continuous monitoring.*

        Our audit determined that the security controls were not tested for 3 of the 22 contractor systems. Of the test results we did receive, we noticed significant variances in quality and consistency. In addition, in FY 2014 OPM required only annual testing of security controls for contractor systems, as opposed to the more frequent testing required for agency-operated systems. OPM's FY 2015 continuous monitoring policy does require more frequent tests for contractor systems, but our preliminary 2015 FISMA audit work indicates that this has not been established.

    b. Since conducting your 2014 audit, have you seen any improvements in OPM's information security controls for managing third-party vendor risks? If so, where have you seen those improvements?

        ***OPM OIG Response**: Since our 2014 audit we have not reported any improvements in OPM's management of third party vendor risks. OPM has informed us that the entire process is currently being revamped and the process relies heavily on security personnel*

that report to the Chief Information Officer as opposed to the OPM program offices – a process that we support.

c. What areas, if any, do you believe are still in need of improvement at OPM?

***OPM OIG Response**: OPM has significant work ahead to develop a mature continuous monitoring program. We also believe the current inspection program for contractor systems could be improved, as it currently stands OPM does not conduct routine inspections/site visits to contractor operated systems.*

2. Does OPM have an inspection program of sub-contractors to third-party vendors?

   a. ***OPM OIG Response**: We are not aware of any such inspection program.*

Questions for Ms. Donna K. Seymour
Chief Information Officer
U.S. Office of Personnel Management

Questions from Representative Michael R. Turner
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

1. As you may know, my Congressional district is home to Wright-Patterson Air Force Base, the largest single-site employer in the State of Ohio. I am concerned that OPM's response to the data breaches does not seek to adequately protect Wright-Patterson Air Force Base personnel whose the personal information may have been compromised as a result of these breaches. Please provide me with the specific steps you are taking to assist these individuals and their families.

We have sent notifications to those affected by the incident involving personnel data. We are offering free identity theft monitoring and restoration services. If an individual was affected by this incident, they have been sent a notice that includes information about the free services available to them for 18 months. As part of this service, they are *automatically* enrolled in:

- **Full service identity restoration, which helps to repair their identity following fraudulent activity; and**
- **Identity theft insurance, which can help to reimburse them for certain expenses incurred if their identity is stolen.**

In addition, we are providing information on our website to educate individuals on ways to protect their identity.

For those affected by the background investigation incident, an online resource, www.opm.gov/cybersecurity, has been created. The site offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.

Impacted individuals will receive a notice in the mail providing details on the incident and the services available to them at no cost for at least three years such as:

- **Full service identity restoration support and victim recovery assistance**
- **Identity theft insurance**
- **Identity monitoring for minor children**
- **Continuous credit monitoring**

- **Fraud monitoring services beyond credit files**

In the coming weeks a call center will be opened to respond to questions and provide more information. If an individual is affected, he or she will not be able to receive personalized information until notifications begin, and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that have questions, and OPM will work with its partners to establish this call center as quickly as possible.

In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

2. Why is the identity theft insurance coverage limited to eighteen months? What processes or analysis led you to conclude that eighteen months was sufficient to protect these individuals?

OPM is offering free identity theft monitoring and restoration services to those affected by the incident involving personnel data. If an individual was affected by this incident, they have been sent a notice that includes information about the free services available to them for 18 months. As part of this service, they are *automatically* enrolled in:

- **Full service identity restoration, which helps to repair their identity following fraudulent activity; and**
- **Identity theft insurance, which can help to reimburse them for certain expenses incurred if their identity is stolen.**

Identity Theft Insurance covers costs associated with identity restoration for up to $1 million. There is no deductible.

A careful and thoughtful analysis of the risk presented by the personnel records incident as well as a review of the services available, precedent, and industry best practices led OPM to conclude that 18 months was the appropriate duration for the comprehensive suite of services offered to help federal employees in the personnel files incident.

3. The information required to be included in the background check Standard Form 86 (SF-86) is extensive. What steps are you taking to assist individuals (relatives, references, etc.) whose information was submitted as part of an SF-86 submission?

There are a number of resources available to assist individuals who information was submitted as part of the SF-86.

- **Currently the following services are being provided to impacted individuals from the personnel records incident:**
    - **Automatic enrollment in identity restoration and theft insurance;**

- **An online cybersecurity resource center at https://www.opm.gov/cybersecurity which offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.**
- **A Congressional hotline, for Members and staff, to assist with questions for their constituents.**
- **An automated phone message providing further information for the federal workforce and the public.**
- **A call center in the coming weeks to respond to questions and provide more information.**

- **Once a notification contract is awarded, and notifications begin to be sent out to impacted individuals, the following additional resources will be available:**
  - **Every individual whose Social Security Number was stolen will receive a notification letter. This letter will be accompanied by an information brochure with information that should be shared with relatives or references who may have been listed on an individual's SF-86 form.**
  - **A comprehensive suite of monitoring and protection services – such as identity restoration support, identity theft insurance, identity monitoring for children, continuous credit monitoring, and additional fraud monitoring services – for at least three years to the applicants and non-applicants with Social Security Numbers and other sensitive information that was stolen.**

This approach builds upon the lessons learned from prior cybersecurity incidents, and ensures that those affected and the public at-large have the information and resources they need to guard against cyber threats. OPM is working as quickly as possible with GSA and DOD on a new contract to notify and provide services for the individuals affected by the background investigation records incident. As part of this process, OPM has benefited from and would like to continue conversations with stakeholders such as Federal employee unions, to hear their feedback and concerns regarding the notification process for the personnel records incident.

Questions for Ms. Donna K. Seymour
Chief Information Officer
U.S. Office of Personnel Management

Questions from Representative Tim Walberg
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

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?

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

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

OPM is moving to a Zero Trust tenet posture. All new architecture use this approach and existing systems are being migrated. These legacy systems were not built to perform at a Zero Trust tenet posture; therefore the migration process will be slower than the build out of new architecture.

OPM continues to explore all opportunities provided by commercial industry leaders. OPM made a decision in mid-2014 that numerous OPM systems would need to be protected at the highest levels. OPM is vigorously pursuing implementation of its target environment. The cyber sprint has significantly influenced OPM, as OPM has significantly influenced the cyber sprints. It is important to note that OPM is in the top quartile of agencies that accelerated use of multi-factor authentication for both

privileged and non-privileged users. OPM is confident in its plan, developed in 2014, but will remain nimble to accommodate advancements in technology or additional needs. We remain committed to a more secure environment.

Questions for Ms. Donna K. Seymour
Chief Information Officer
U.S. Office of Personnel Management

Questions from Representative Steve Russell
Committee on Oversight and Government Reform

June 24, 2015 Full Committee Hearing titled: "OPM Data Breach: Part 2"

1. What data specifically was breached pertaining to SF-86 files? Was it just the form specifically, or full background investigation notes?

Social Security numbers (SSNs) and other sensitive personally identifiable information (PII) was stolen for anyone who underwent a background investigation by submitting an SF-86, SF-85P or SF-85 form, and non-applicants such as spouses and co-habitants whose SSN and other sensitive PII were provided by the applicant. Identifying information in these records about applicants include details such as SSNs, residency and educational history, employment history and activities, information about immediate family and other personal and business acquaintances, health, criminal and financial history, and other details. Also, information recorded during the investigation process was stolen for some applicants. Beyond the information on an individual's SF-86 or 85, some background investigation records also include findings from interviews conducted by background investigators and include fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen. While background investigation records do contain some information regarding mental health and financial history provided by those that have applied for a security clearance and sources contacted during the background investigation, there is no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of Federal personnel were impacted by this incident (i.e. annuity rolls, retirement records, USA JOBS, Employee Express).

2. What steps has OPM taken to protect the identity and credit of family members, including spouses, dependents, and cohabitants whose information was breached by the loss of SF-86 data? Will OPM extend the same identity theft protections to those individual as they have to federal employees?

OPM is taking the following steps to assist Federal employees and other individuals:

1. **Providing a comprehensive suite of monitoring and protection services – such as identity restoration support, identity theft insurance, identity monitoring for children, continuous credit monitoring, and additional fraud monitoring services – for at least three years to the to any individuals whose Social Security Numbers was stolen during this cyber incident. In most cases,**

minor children's social security number was not included on the SF-86 form; however due to the risk associated with identify theft of minors, all impacted applicants will have the option of signing up a current minor children whose information was listed on the background investigation form for identity theft monitoring services.

2. **Every individual whose Social Security Number was stolen will receive a notification letter. This letter will be accompanied by an information brochure with information that should be shared with relatives or references who may have been listed on an individual's SF-86 form.**
3. **Establishing an online cybersecurity resource center at https://www.opm.gov/cybersecurity which offers information about the incident, identifies what groups of individuals that are most likely impacted, describes the services available to impacted individuals, provides concrete action steps that individuals can take to protect themselves from cyber breaches, and answers a number of additional frequently asked questions. The site also includes the capability for individuals to sign up for alerts via RSS feed.**
4. **Establishing a call center in the coming weeks to respond to questions and provide more information. In the interim individuals are encouraged to visit https://www.opm.gov/cybersecurity.**
5. **Explore a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future.**

This approach builds upon the lessons learned from prior cybersecurity incidents, and ensures that those affected and the public at-large have the information and resources they need to guard against cyber threats. OPM is in the contracting process for a Vendor and will be sharing information regarding the contracting process at a later date.

3. There have been press reports of OPM records showing up for sale on the darknet, though other reports indicating those records may in fact be from a separate breach of a different government agency. At this time, do we know if any documents from the OPM breach have shown up for sale anywhere?

There is no information at this time to suggest any misuse or further dissemination of the information that was stolen from OPM's systems.

4. Is it normal for an adversary to have this type of information for so long and not offer it for sale?

This is a matter best addressed by the intelligence community.

5. If this information is not offered for sale, does that point to counterintelligence as they likely motive behind the attacks?

These questions are best answered by the Intelligence Community.

Question#:	1
Topic:	OPM records
Hearing:	OPM Data Breach: Part II
Primary:	The Honorable Jason Chaffetz
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

2015-07-14 Barron-DeCamillo-DHS QFRs RESPONSE

Question: There have been press reports of OPM records showing up for sale on the darknet, though other reports indicating those records may in fact be from a separate breach of a different government agency. At this time, do we know if any documents from the OPM breach have shown up for sale anywhere?

Response: No. At this time we have not discovered any documents from this breach for sale.

Question: Is it normal for an adversary to have this type of information for so long and not offer it for sale?

Response: I defer to the Director of National Intelligence [or the F.B.I.] with respect to trends and patterns on sale of stolen information.

Question: If this information is not offered for sale, does that point to counterintelligence as they likely motive behind the attacks?

Response: I defer to the Director of National Intelligence.