SECURITY CLEARANCE REFORM: THE PERFORMANCE ACCOUNTABILITY COUNCIL'S PATH FORWARD

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

FEBRUARY 25, 2016

Serial No. 114–105

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

23–404 PDF WASHINGTON : 2017

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

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

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

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

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
JACK THORLIN, *Counsel*
WILLIAM MARX, *Clerk*

CONTENTS

SECURITY CLEARANCE REFORM: THE PERFORMANCE ACCOUNTABILITY COUNCIL'S PATH FORWARD

Thursday, February 25, 2016

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

The committee met, pursuant to call, at 9:59 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Mica, Duncan, Jordan, Walberg, Amash, DesJarlais, Massie, Meadows, Buck, Walker, Blum, Hice, Russell, Carter, Hurd, Palmer, Cummings, Maloney, Norton, Lynch, Connolly, Duckworth, Lawrence, Lieu, Plaskett, DeSaulnier, and Welch.

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

I appreciate you all being here for this hearing, "Security Clearance Reform: The Performance Accountability Council's Path Forward."

At last count, the Director of National Intelligence reported 4.5 million people held security clearances, 4.5 million, and the queue for clearances continues to grow. At the end of fiscal year 2015, there were more than 388,000 new background investigations, and 117,000 periodic reinvestigations backlogged at the Office of Personnel Management. That is a lot of folks with access or requesting access to our most sensitive national security information.

And we have learned last year that most if not all the personal information collected during background investigations was exfiltrated in one of our country's biggest cyber attacks. We have to be careful not to ever, ever allow that to happen again. We have to fix the process, and we have to protect the information we collect.

And as part of my opening statement, I would actually like to yield some time to the gentleman from Oklahoma, who has been very keenly involved in this, Mr. Russell.

Mr. RUSSELL. Thank you, Mr. Chairman.

And I do appreciate the panel also being here today.

Following the June 2015 OPM data breach, I began working with my good friend and colleague Congressman Ted Lieu on a path forward that would protect not just the personal and private information of those who hold security clearances but what amounts to crown jewels for any foreign intelligence service.

My concern deepened as we learned the full extent of the breach. All told, 18 million records were stolen in the breach, including data on military and intelligence personnel, placing Americans at great risk that has not abated.

I also received a letter from my time in the service being a former top secret SCI clearance holder in the military stating that my data had been compromised. For me and my friend Congressman Ted Lieu, who also received a letter, this is not some academic issue.

It should also be noted that the DOD never lost security of such data when it was under their care. It was through pressure, largely from Congress, to save money, make an effort to eliminate a large backlog. Well, we eliminated the backlog by eliminating security. Whatever savings we had has surely been forfeited in that result.

Today, we will examine the reform efforts advanced by the 90-day sustainability and security review by the Performance Accountability Council, or PAC. One of the main points of emphasis I made along with Mr. Lieu was the need for the Department of Defense to own the data for our service members and Department civilians. And I am encouraged that the PAC review will result in this being accomplished.

Under the reforms recommended by the PAC, the Department of Defense will be responsible for not just building the infrastructure that will house this critically important data; they will also be responsible for defending it.

The questions remain, however, that while the DOD has been given the responsibility, will they be given the authority while being placed under a bureau that is placed under a department? This has to be answered.

I remain concerned regarding the creation of the new National Background Investigations Bureau, or NBIB. NBIB will ultimately absorb the Federal Investigative Service, which currently is tasked with conducting background investigations for the vast majority of our government. And while I believe we all recognize the pressing importance and urgency of modernizing and updating the security clearance process, I remain unconvinced that allowing an OPM entity, whether its name be FIS or NBIB, is the correct path in the long term. After all, the OPM allowed the worst breach of secure data in our nation's history.

I hope that today's hearing will show by NBIB will be a new way forward rather than just a rebranding of FIS. I appreciate the willingness of Acting Director Cobert and other members of the PAC that they have shown in working with me and Congressman Lieu on this issue and your willingness to give us complete access and answer our questions.

My aim in this hearing, as I hope we will hear today with the chairman's indulgence, is to ensure that the process forward for NBIB is the right path and that we are not just putting a fresh coat of paint on a house with a bad foundation, a house that our enemies have broken into and stolen everything in it, I might add.

I look forward to hearing from our panel of witnesses as we seek to understand the difference between NBIB and its predecessor, as well as the role of the Department of Defense in protecting this vital information.

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

Chairman CHAFFETZ. I thank the gentleman.

In the essence of time, I will submit the remainder of my opening statement into the record.

Chairman CHAFFETZ. I now recognize the ranking member, the distinguished gentleman from Maryland, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. And I want to thank you for holding today's hearing. I commend both Congressman Lieu and Russell for their work on this issue and for requesting today's hearing.

I would like to yield 2 minutes to the gentleman from California, Mr. Lieu.

Mr. LIEU. Thank you, Ranking Member Cummings, for giving me the opportunity to speak. And I want to thank the chair and the ranking member for holding this hearing, as well as last year's hearings, that exposed fundamental weaknesses in our nation's cybersecurity, particularly as applied to OPM.

And last year's OPM data breach was the most significant government cybersecurity breach we have ever uncovered and serves as a poignant reminder that U.S. Government needs to change the culture of cybersecurity.

It also revealed that there was an irrational system where we had a human resources agency protecting these critical national security assets or security clearance records, and as Representative Russell mentioned, not only did we both get notices that our information was compromised, I think our spouses did as well.

In October 7 of last year, Congressman Russell and I wrote a letter to the administration. It was to the Performance Accountability Council requesting that you transfer the security clearance data, the protection and design of it, to a Department of Defense agency. The letter was dated October 7, and, Mr. Chairman, I would like to enter it into the record.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LIEU. I am pleased that the administration and the PAC board has in fact now put forward a plan that will transfer the design and protection of this information to a DOD agency.

I do share the same concerns that Congressman Russell has regarding the NBIB. I would like to know why it is we need the creation of a new bureau, how it would be different from the Federal Information Service, and whether the lines of authority are clear, and if there is going to be accountability.

And I agree with Congressman Russell that we need to hear about how these reforms are not just going to be window dressing on a broken home but a comprehensive renovation.

And let me again thank the witnesses here today for your public service, for your hard work on this issue, and look forward to working with you to make our nation's cybersecurity stronger.

I yield back.

Mr. CUMMINGS. Again, I want to thank Representative Lieu and Representative Russell for their leadership on this issue.

And, Mr. Chairman, this is precisely the type of hearing our committee should be having, looking across agencies at new proposals to improve the effectiveness and efficiency of government.

Mr. Chairman, in 2013, a very disturbed Navy contractor with a security clearance shot and killed 12 people and injured four others here in Washington, D.C. Our committee conducted an investigation of that terrible shooting, and we found that a contractor USIS conducted the shooter's background check. We found that USIS failed to include information on his previous arrest for shooting out the tires of his neighbor's car. As a result, he was given a secret-level security clearance.

We also found that USIS committed fraud against the American taxpayers on a much wider scale by submitting incomplete background investigations. USIS ultimately agreed to the demands of the Justice Department to forego $30 million as a result of its actions, and it no longer conducts background checks on behalf of the Federal Government.

I ask unanimous consent that the report I issued on this topic be entered into the record.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. CUMMINGS. Thank you, Mr. Chairman.

Then, last year, cyber attackers successfully breached OPM's data systems. Again, our committee investigated, and again, we found a weak link in the chain: a contractor. We heard testimony explaining that these cyber attackers were able to gain access to Federal systems by using KeyPoint's privileged access to OPM's networks. As a result, the personal information of millions of Federal employees with security clearances was compromised.

These cyber attacks on OPM were not isolated incidents. Other Federal contractors, including Anthem and Premera, were also attacked. Experts believe these were all part of a sophisticated, coordinated cyber espionage campaign. They all occurred at about the same time, they all targeted sensitive information about Federal employees, and they all were carried out using similar malware.

The proposal we are discussing today is a significant and substantive response to these events, and it is more than just the new National Background Investigations Bureau. The administration's proposal leverages the expertise of key parts of the government like the Department of Defense to provide critical IT and cybersecurity capabilities.

I believe this is a serious effort to combat sophisticated cyber attackers who are targeting our government, and it deserves serious consideration by this Congress.

Today, I want to hear more about how this proposal will address the significant problems we have had with these contractors. The government's reliance on contractors helps supplement their workforce and increase our capabilities, but as we have seen, it also carries major risks. I want to know how the administration's proposal will increase oversight and accountability over contractors charged with safeguarding some of our nation's most sensitive information.

Let me address two final points. First, earlier this week, Donna Seymour, OPM's chief information officer, retired after more than 35 years of service to our great country. Unfortunately, some have inaccurately—inaccurately—blamed Ms. Seymour for preexisting vulnerabilities she inherited. Now, I was one of the most vocal critics of the CIO's office at our last hearing because the inspector gen-

eral raised concerns about obtaining access to information from that office. And I continue to believe those concerns were valid.

However, our investigation has now found that the cyber attacks against OPM were already underway when Ms. Seymour took office in December of 2013. In addition, experts in and out of the agency informed us that she helped uncover the attack, she led an aggressive response, and she elevated cybersecurity to a top priority when previously it had language.

Finally, Mr. Chairman, I want you to know that I believe that these recent political attacks against Ms. Seymour are both unfair and inaccurate. They also set a terrible precedent that would discourage qualified experts from taking on the challenges our nation faces in the future.

Finally, on that same note, as we sit here today, certain Republicans in the Senate are holding up the nomination of a great public servant, Beth Cobert as OPM Director, for political reasons that have nothing, absolutely nothing to do with her qualifications for the position. As we all know, Republicans are threatening to block anyone the President nominates to the Supreme Court for political reasons in the same way they are stalling Ms. Cobert's nomination, despite the fact that she has been widely praised for turning things around at the agency.

I have said it before and I will say it again: We must not only reach common ground, we must reach higher ground. And that is what the American people are demanding of us, and that is why they are so frustrated. Just this morning, Senator David Vitter issued a press release proclaiming that he is "blocking Beth Cobert to be Director of the Office of Personnel Management" as if he is bragging about it. He is doing this because of his political opposition to the Affordable Care Act and not for anything relating to the actions of Ms. Cobert.

I have a copy of the press release here, and I ask unanimous consent that it be entered into the record, Mr. Chairman.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. CUMMINGS. As I close, this is simply outrageous. The inspector general has praised her efforts, and even some of her critics in Congress have praised her leadership. There is absolutely no reason to continue playing politics, and I hope that every member of our committee will join me today in asking the Senate to confirm President Obama's nomination for this position as soon as possible.

Mr. Chairman, again, I want to thank you for your indulgence. I want to thank you for calling this very important hearing, and I look forward to the testimony of our witnesses.

And with that, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

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

As we introduce this first panel of witnesses, I want to particularly thank Ms. Cobert, who has been nominated by the President to be the new Director of the Office of Personnel Management. I find her to be a very competent person who is a breath of fresh air who actually has the background to run this agency.

Part of the reason we got into this mess, since you brought it up, to the ranking member, is that there was a political appointee that

was put in there who had no business running the Office of Personnel Management. She was terribly under-qualified to do this, and I am glad that the agency has taken action to get rid of what I consider to be one of the worst problems, which was their CIO because there were undoubtedly problems, but that was in my personal opinion not part of the solution.

Now, that has been taken care of, and we can further debate that. That is not the subject of the hearing today. What I appreciate is the communication from Ms. Cobert. I think she has, as I said, the right background. We do still need some responsiveness relating to a subpoena, but I do believe that the Office of Personnel Management is making an effort to get that information to us.

I want to be one that is counted as supporting her nomination, and I think the country will be better off, the government will be better off confirming her presence and allowing her to be the Director, fully confirmed, as soon as possible.

Mr. CUMMINGS. Mr. Chairman, would you yield for just ——

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS.—30 seconds?

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Would you join me in a letter today to send to Senator Vitter saying what you just said?

Chairman CHAFFETZ. I will send one to the majority leader ——

Mr. CUMMINGS. All right.

Chairman CHAFFETZ.—but ——

Mr. CUMMINGS. That will do.

Chairman CHAFFETZ.—I don't want to send one to a specific ——

Mr. CUMMINGS. Fine.

Chairman CHAFFETZ. But ——

Mr. CUMMINGS. I would appreciate that.

Chairman CHAFFETZ.—I am saying it publicly. I will put it in writing. I believe Ms. Cobert has the right qualifications. I think the country and the office will be better off with her confirmation.

Mr. CUMMINGS. I just wanted to make sure we did it together if we can.

Chairman CHAFFETZ. Yes.

Mr. CUMMINGS. Thank you very much.

Chairman CHAFFETZ. And so that is quite the introduction to joining us here today. We do appreciate your presence and your expertise and look forward to hearing how we move forward, but again, I am glad that there have been changes in the CIO's office. That is part of the solution and gets rid of the problem.

Mr. Terry Halvorsen, who is the chief information officer at the United States Department of Defense, welcome here, sir. Thank you.

Mr. Tony Scott, Deputy Director for Management at the U.S. Office of Management and Budget, we appreciate your presence as well; and Mr. William Evanina, did I pronounce that—yes, I hope so. Thank you. The Director of National Counterintelligence and Security Center at the Office of the Director of National Intelligence. We appreciate your presence as well.

All of these panel members have very important, critical roles to the safety and security of our nation. We thank you for participating.

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

[Witnesses sworn.]

Chairman CHAFFETZ. Thank you. The witnesses may be seated. Let the record reflect that all of them answered in the affirmative.

In order to allow time for robust discussion and questioning by members, we would appreciate it if you would limit your verbal comments to 5 minutes. Your entire written statement will be submitted into the record.

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

WITNESS STATEMENTS

STATEMENT OF BETH COBERT

Ms. COBERT. Chairman Chaffetz, Ranking Member Cummings ——

Chairman CHAFFETZ. Sorry, microphone there. Yes, thank you.

Ms. COBERT. Get that right. Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify before you today.

This year, the administration announced significant changes to how the Federal Government performs background investigations. As a result, OPM will stand up the National Backgrounds Investigations Bureau, NBIB. The NBIB will absorb the operations of OPM's Federal Investigative Services and will be housed within OPM. The NBIB will be a new government-wide service provider for background investigations. OPM has and will work closely with their interagency partners on this effort that is so critical to the integrity of the Federal workforce and our national security.

The NBIB presents significant change for the Federal Government in a number of important and positive ways. DOD will design, build, and operate the NBIB's investigative IT systems in coordination with the NBIB. This strengthens the Federal Government's security clearance and background investigation processes by leveraging DOD's significant IT, national security, and cybersecurity expertise.

NBIB will also have elevated standing and prominence within the national security leadership across the government. The head of NBIB will be a Presidential appointee and a full member of the Suitability and Security Clearance Performance Accountability Council, the PAC. Additionally, NBIB will have its own dedicated structures in vital areas of operations tailored to NBIB's core mission.

Finally, we will institutionalize NBIB's ability to tap into the rich expertise and knowledge that exist across the Federal Government through locating the leadership team in Washington, D.C., and utilizing programs such as rotating details and joint-duty assignments.

OPM plays an important role in conducting background investigations for the vast majority of the Federal Government. Currently, OPM's Federal Investigative Services conducts investigations for over 100 Federal agencies, approximately 95 percent of the total background investigations government-wide, including more than 600,000 national security investigations and 400,000 in-

vestigations related to suitability, fitness, or credentialing each year.

The NBIB will assume the investigative functions of OPM's Federal Investigative Services and add important new capabilities. The NBIB will concentrate solely on its mission to provide effective, efficient, and secure background investigations for the Federal Government. The NBIB will receive dedicated support in key areas, including acquisition and privacy, and will focus on bringing in additional talent with national security expertise as we do so.

To begin the implementation phase of these reforms, we are establishing a transition team. This team, comprised of personnel from the PAC member agencies, will be established by mid-March. Supporting the implementation of the NBIB and aiding its success will be a core focus for the PAC. The NBIB will leverage existing expertise, resources, and processes for providing government-wide services as it is launched.

The NBIB will work closely with OPM's Federal Investigative Services leadership to minimize disruption for agencies that rely on us to perform background investigations. We are working along with DOD to establish an initial transition schedule to sunset the OPM IT systems currently supporting background investigations.

Throughout these efforts, we will provide continuity of service to our customer agencies by providing quality background investigation services. Our goal is to have the NBIB's initial operating capability officially established with a new organizational design and a leader in place by October 2016.

The establishment of the NBIB continues this administration's work to protect American citizens and some of our nation's most sensitive information and facilities. On behalf of OPM, I am proud to be part of this most recent effort by the administration. I look forward to working with my colleagues on this panel, with our customer and partner agencies across the Federal Government, and with this Congress in a bipartisan, collaborative fashion for the benefit of the American people. I'm happy to answer any questions you may have. Thank you.

[Prepared statement of Ms. Cobert follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

TESTIMONY OF
BETH F. COBERT
ACTING DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

"Security Clearance Reform: The Performance Accountability Council's Path Forward"

February 25, 2016

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

Thank you for the opportunity to testify before you today about ongoing developments in how the Federal Government conducts background investigations. Last year, in light of increasing cybersecurity threats and incidents, the 13-agency Suitability and Security Clearance Performance Accountability Council (PAC) initiated an inter-agency Suitability and Security Review (the 'Review') that sought the advice of experts within and outside government to seek ways to best secure the sensitive data collected as part of background investigation processes and modernize this critical governmental function so that its governance, workforce and business processes meet higher performance standards. The inter-agency group was tasked with developing additional enhancements to further secure Federal information and strengthen the systems supporting background investigation processes, as well as with re-examining reforms.

The Review's recommendations not only followed this recent inter-agency effort, but are also informed by the work conducted in the 120 Day Review and its resulting Report following the tragic events at the Washington, DC Navy Yard. The questions contemplated in the Review's recommendations have been considered carefully, in great detail, and are, in my view, a strong step forward. The Review's recommendations further strengthen existing reform activities, including the issuance and implementation of new training standards for investigators and adjudicators; the implementation of new investigative standards; and the development and

issuance of Federal standards for assessing the quality of national security and suitability background investigations government-wide.

As a result of the Administration's continued examination of possible reforms to background investigation processes, the Review concluded that there was a need to make further reforms to the background investigation function that would build upon the efforts already underway. In January of this year, the Administration announced a framework for strategic and structural changes to modernize and fundamentally strengthen how the Federal Government performs background investigations. OPM has and will work closely with our interagency partners on this effort that is so critical to the integrity of the Federal workforce and our Nation's security. In conjunction with this effort, the Office of Personnel Management (OPM) will stand up a new government-wide service provider for background investigations, the National Background Investigations Bureau (NBIB), which will be housed within OPM.

Pursuant to that strategy, the Department of Defense (DOD), with its unique national security perspective, will design, build, secure, and operate the NBIB's investigative IT systems in coordination with the NBIB. As part of developing the timeline for transition, we are working along with DOD to establish an initial schedule to sunset the OPM IT systems currently supporting background investigations.

The NBIB will concentrate solely on its mission to provide effective, efficient, and secure background investigations for the Federal Government. The NBIB will receive dedicated support in key areas including acquisition and privacy – and we will focus on bringing in additional talent with national security expertise as we do so. The NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up and new IT systems are developed. The head of the NBIB will be a Presidential appointee and will be elevated to become a full member of the PAC, allowing us to synchronize both the policy and operational functions related to background investigations.

OPM plays an important role in conducting background investigations for the vast majority of the Federal Government. Currently, OPM's Federal Investigative Services (FIS) conducts investigations for over 100 Federal agencies – approximately 95 percent of the total background investigations government-wide – including more than 600,000 national security investigations and 400,000 investigations related to suitability, fitness, or credentialing each year. The NBIB will assume this mission and absorb the investigative functions of FIS and add important new capabilities. The NBIB leadership will be headquartered in Washington D.C., which will facilitate smooth and efficient coordination with interagency partners.

This represents significant change because it will modernize the Federal Government's security clearance and background investigation processes; leverage DOD's significant IT, national security and cybersecurity expertise; fully align the head of the NBIB as a Presidential appointee

and full member of the PAC; and provide the needed operational flexibility and dedicated support structures for specialized skills while also maximizing OPM's organizational structure for generalized administrative support.

To begin the implementation phase of these reforms, we are establishing a transition team to oversee and manage this transition. This team, composed of personnel from PAC member agencies, will be established by mid-March and will be responsible for creating a comprehensive implementation group to support standing up the NBIB that works closely with FIS leadership to ensure minimal disruption for agencies that rely on us to perform background investigations. Our goal is to have the NBIB's initial operating capability officially established with a new organizational design and leader by October 2016, though implementation work will remain to be done after this date. The transition team will focus on five main areas of work: Business Process Analysis and Reengineering; Resource Management; Information Technology and Cybersecurity; Mission Support; and Change Management.

The NBIB will leverage existing expertise, resources, and processes for providing government-wide services as it is launched. OPM is establishing an internal transition team as well, which will work closely with the interagency team. And there are other steps OPM is taking to push forward progress in the near term. We are on our way to awarding a new background investigations fieldwork contract, on which we worked on closely with our interagency partners including DOD. Throughout these efforts, we will provide continuity of service to our customer agencies providing quality background investigative services.

In close coordination with our agency partners, OPM continues to make progress on strengthening our cybersecurity posture. For example, OPM has implemented the enforcement of Personal Identity Verification cards for two-factor authentication for network access. OPM has increased the number of scans that allow us to review the entire OPM network for signs of compromise. OPM has worked with our interagency partners to patch critical vulnerabilities, tighten policies and practices for privileged users, and conduct reviews of our high value asset systems. Finally, OPM has hired a new Acting Chief Information Security Officer, four new SES-level employees, and four new senior IT program managers to further strengthen the senior IT team, as well as a new senior cyber and information technology advisor to support the ongoing response to recent incidents, complete development of OPM's plan to reduce the risk of future incidents, and recommend further improvements to secure OPM's IT. These steps build on efforts the Administration has taken through the 30-day Cybersecurity Sprint and the release of both the Cybersecurity Strategy and Implementation Plan and the Cybersecurity National Action Plan to increase our cybersecurity capabilities and protect systems and data government-wide.

Supporting the implementation of the NBIB and aiding its success will be a core focus for the PAC. The PAC will monitor the NBIB's performance in order to identify, propose, and help drive enterprise-level process enhancements. The PAC will make recommendations for changes

to Executive Branch-wide guidance and authorities to resolve overlaps or close policy gaps where they may exist and facilitate data-driven, transparent policy-making processes. The PAC and the Performance Improvement Council will also develop, implement, and continuously re-evaluate and revise outcome-based metrics that help measure the effectiveness of the vetting processes (e.g., security, investigative and adjudicative quality, cost, timeliness, reciprocity, customer service, and other performance characteristics).

The establishment of the NBIB continues this Administration's efforts to improve how the Federal Government performs background investigations to protect American citizens and some of our Nation's most sensitive information and facilities. In partnership with the Director of National Intelligence (DNI), we have established a five-year reinvestigation requirement for all individuals in positions of public trust, as well as those with a security clearance, regardless of the level of access, and reduced the number of individuals with active security clearances. In addition, we support the DNI's efforts launching programs to continuously evaluate personnel with security clearances to determine whether they continue to meet the requirements for eligibility; and developed recommendations to enhance information sharing from State, local, and Federal law enforcement entities when conducting background investigations.

On behalf of OPM, I am proud to be a part of this most recent effort by the Administration, and I look forward to working with my colleagues on this panel and with this Congress in a bipartisan, productive fashion for the benefit of the American people. I am happy to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

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

STATEMENT OF TERRY HALVORSEN

Mr. HALVORSEN. Good morning, Mr. Chairman, ranking member, and distinguished members of the committee. Thank you for this opportunity to testify before the committee today on DOD's information technology and cybersecurity support to the National Background Investigation Bureau.

In duly capacity, I look forward to expanding this role with the opportunity to oversee IT systems for the National Background Investigation Bureau. This is an opportunity for the Federal Government to truly capitalize on established DOD technology, commercial expertise, other government expertise to improve the security of the IT infrastructure for the vital Federal background investigation system process.

DOD has substantial experience in the development of systems with strong cybersecurity and has worked to integrate commercial- and government-developed cyber defense and detection tools into the DOD networks. This gives the Department unique cyber defense capabilities.

The DOD is driving cultural, business, and technical innovation into DOD by better integrating our IT infrastructure, supporting agile and innovative IT. We will do the same here.

The Department's cybersecurity workforce is well trained to protect against and respond to cyber intrusions. Our cybersecurity operations and procedures are mature and reinforced by policy and regulations across the Department.

We will bring together the Department's full range of resources and expertise. The Defense Information Systems Agency will oversee the organization's effort to provide the IT services and security with continual oversight by my office in my role as the CIO.

The Department's objective, of course, is to replace the current background investigation information systems with a new, more reliable, flexible, and secure system in support of the NBIB while we ensure continuous operations for the vital background investigations system and ensure that we are making as much security improvements to the current systems while we are in the process of replacing them.

I echo Beth's comments. We have been working closely together with OPM and other parts of the government since this incident was discovered. We will continue to do so.

DOD will cooperatively conduct a full cybersecurity assessment of the current background investigations infrastructure. This joint assessment will determine the near-term steps that the Department will take to assist OPM with the operation of the current system, as well as to develop the steps that OPM itself can take to better defend the current systems as we are designing and putting in of the new investigation systems IT infrastructure.

I will stress again we will do this in cooperation with everyone, but in the end, DOD has the technical responsibility and the technical expertise to oversight what we are doing in this new IT investigation system.

Thank you, and stand by for your questions.

[Prepared statement of Mr. Halvorsen follows:]

STATEMENT BY

TERRY HALVORSEN
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

BEFORE THE

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

ON

SECURITY CLEARANCE REFORM: THE PERFORMANCE ACCOUNTABILITY COUNCIL'S PATH FORWARD

FEBRUARY 25, 2016

NOT FOR PUBLICATION UNTIL RELEASED BY THE HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

Introduction

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for this opportunity to testify before the committee today on the Department's Information Technology and Cybersecurity support to the National Background Investigation Bureau. I am Terry Halvorsen, the Department of Defense (DoD) Chief Information Officer (CIO). As the senior civilian advisor to the Secretary of Defense for IT, I am responsible for all matters relating to the DoD information enterprise, including cybersecurity for the Department. In this capacity, I look forward to expanding this role with this opportunity to oversee IT systems for the National Background Investigations Bureau (NBIB). This is an opportunity for the Federal Government to truly capitalize on established DoD technology and expertise to improve the security of the IT infrastructure for the vital federal background investigation systems process. DoD has substantial experience in the development of systems with strong cybersecurity, and has worked to integrate commercial and government developed cyber defense and detection tools into the DoD networks, which gives the Department unique cyber defense capabilities.

The DoD CIO is driving cultural, business, and technical innovation in the DoD by better integrating our IT infrastructure, streamlining business processes, and supporting agile and innovative IT acquisition. The Department's cybersecurity workforce is well trained to protect against and respond to cyber intrusions. DoD cybersecurity operations and procedures are mature and reinforced by policy and regulations across the entire Department. DoD's IT development process requires the inclusion of cybersecurity in every step of the development lifecycle of all systems, even after the system is fielded. The Department's processes, systems, and security architecture are well-integrated and continuously improving to ensure that future attacks are deterred or detected quickly and effectively. DoD will use these same processes to build IT support for the NBIB.

As the lead for building the new background investigation IT system, I will bring together the Department's full range of resources and expertise. LTG Alan Lynn, Director of the Defense Information Systems Agency (DISA), will oversee his organization's efforts to provide the majority of IT services and security to the NBIB, under DoD CIO oversight. The Department's objective is to replace the current background investigations information systems with a new and more reliable, flexible, and secure system in support of the NBIB. Ensuring continuous operations for the vital background investigations system, even as we build and transition to the new IT infrastructure, is paramount.

DoD has been working closely with OPM since the incident was discovered. Recent collaboration has focused on getting the Department's team prepared to begin the process of designing, building, operating, securing, and defending these IT systems. DoD will support OPM as they continue to operate the current system. DoD will cooperatively conduct a full cybersecurity assessment of the current background investigation

infrastructure. This joint assessment will determine the near-term steps that the Department can take to assist OPM with the operation of the current system, as well as near-term steps that OPM itself can take to better defend the current system. It will also inform DoD's design and instantiation of the new investigation system IT infrastructure. DISA will lead this assessment, with support from the NSA and the Deputy CIO for Cybersecurity. Planning for this assessment is ongoing, with on-site work at OPM expected to begin within the next 60 days.

In mid-December, DoD CIO formed a multi-organizational IT Task Force with members from OPM, DISA, NSA, USD(I), and DMDC to build the foundation for future program office and acquisition activities. This IT Task Force has six work streams to articulate the detailed requirements and design of the new information system and the supporting operations. The work streams are: Data Strategy; Application Migration / Business Process Reengineering; Architecture; Governance; Operations; and Resource Management/Program Management. The IT Task Force will analyze the current OPM system and all of its dependencies in detail, scope the new system architecture requirements, and draft implementation and operations plans with metrics for the new system.

As the organization responsible for providing the majority of the IT support directly to the NBIB, DISA will lead development and deployment of the new information system. DISA also will operate and defend the system, under the operational control of USCYBERCOM. The full scope of DoD cyber tools, including those that integrate government and commercial technology, such as the Joint Regional Security Stacks, will protect the systems as they are developed and fielded within the DoD network. DISA cyber operations personnel will conduct monitoring, incident detection, diagnostics, and adversary containment. Then, DISA – supplemented as necessary by USCYBERCOM Cyber Protection Teams – will handle incident response and remediation. The alignment of NBIB systems under the DoD will assure that we leverage all of this national security systems expertise and capability to protect the background investigation data.

Conclusion

In closing, the Department is excited about this opportunity to design, develop, secure, and operate, and defend the new background investigation IT systems for the NBIB. This is an important opportunity for the Federal Government to truly capitalize on established DoD technology, expertise, and information technology systems to improve the security of the IT infrastructure for the vital federal background investigations process. I want to thank you for your interest in our plans to support NBIB, and I look forward to your questions.

Chairman CHAFFETZ. Thank you.

Mr. Scott, I incorrectly identified your title. You are actually the U.S. chief information officer. My apologies for that. But you are now recognized for 5 minutes.

STATEMENT OF TONY SCOTT

Mr. SCOTT. Thank you, Chairman Chaffetz. I was grateful for the promotion, but my boss would probably be angry about that.

So, Chairman Chaffetz, Ranking Member Cummings, and members of the committee, thank you for the opportunity to speak about the administration's recently announced changes to modernize and strengthen how the Federal Government performs and safeguards background investigations for its employees and contractors.

As you know, the Federal Government issues, handles, and stores important and sensitive data, and we use this data to conduct critical government functions, one of which is the subject of today's hearing, the Federal Government's background investigations process.

As we all know, as technology evolves and our economy becomes more digitally connected, the Federal Government's tools, systems, and processes for managing sensitive data and for conducting background investigations must also evolve. And to protect the personal data of our employees and citizens, we must keep pace with the technology advancements that occur in order to anticipate, detect, and counter external and internal attempts to breach government systems.

In my role as Federal chief information officer, I'm particularly concerned with confronting the unyielding cybersecurity threats posed to the information technology systems used across the Federal Government. My team is responsible for developing and overseeing the implementation of Federal IT policy through a variety of responsibilities. Today, I'll focus on the Administration's response to increasing cybersecurity threats and actions we are taking to improve the government's background investigation process through the establishment of the new National Background Investigations Bureau, or NBIB.

In 2008, the interagency sustainability—or Suitability and Security Clearance Performance Accountability Council, or the PAC as we call it, was established through an Executive order. The PAC is convened and chaired by the Office of Management and Budget and consists of the Director of National Intelligence, the Director of the U.S. Office of Personnel Management, and the Departments of Defense, Treasury, Homeland Security, State, Justice, and Energy, and the FBI, among other agencies.

The PAC oversees reforms to the process—or to the processes on which Federal agencies and the public rely to ensure that Federal employees, contractors, and members of the armed forces are suitable for employment and can be trusted with access to facilities and sensitive information.

As Beth mentioned, the administration will establish a new Federal entity, the National Background Investigations Bureau, to modernize and strengthen the government's background investiga-

tion processes. That will include organizational redesign led by a political appointee, who will be a full member of the PAC.

It will include reengineering efforts to look at underlying business processes. DOD will design, build, secure, and operate NBIB's IT. This will leverage DOD's expertise in IT and cybersecurity while better protecting sensitive information and will deploy the fullest security resources against increasingly sophisticated and evolving threats.

To support this work, the President's fiscal year 2017 budget includes $95 million within DOD's top line that will be dedicated to the development of these IT capabilities.

The PAC will establish an interagency cybersecurity advisory group to provide advice and counsel on system development and threat mitigation, and these efforts are consistent with OMB's direction to all Federal agencies to modernize their IT systems to adequately secure mission functions, systems, and information. And a dedicated privacy official will be appointed to advance privacy by design as new processes and systems are developed.

More broadly, enhanced cybersecurity across all Federal agencies will be strengthened by the implementation of the Cybersecurity National Action Plan, or CNAP, which builds on the security measures and initiatives that have been implemented in response to the 2015 cyber incidents. The CNAP takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections and begin the long-overdue replacement of legacy systems while ensuring privacy and maintaining public safety and economic and national security.

We look forward to working with Congress to create a more secure, efficient, and effective Federal backgrounds investigations infrastructure. I thank the committee for holding this hearing and pleased to answer any questions you may have.

[Prepared statement of Mr. Scott follows:]

Embargoed until Delivered

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

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

February 25, 2016

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, I appreciate the opportunity to appear before you today to speak about the important issue of the Administration's recently announced changes to modernize and strengthen how the Federal Government performs and safeguards background investigations for its employees and contractors.

As you know, the Federal Government is responsible for issuing, handling, and storing important and sensitive data. We are also responsible for using this data as part of many different critical functions, one of which is the subject of today's hearing – the Federal Government's background investigations process.

As the world's technologies continue to evolve and our economy becomes ever more digitally connected, the Federal Government's tools, systems, and processes for managing this sensitive information and for conducting background investigations must also evolve. We must keep pace with technological advancement in order to anticipate, detect, and counter malicious attempts to breach Government systems, and to address threats posed by trusted insiders who may seek to do harm to the Government's personnel, property, and information systems.

Given the numerous Information Technology (IT) systems that are used across government, and the amount of data that is collected to conduct background investigations, confronting the cybersecurity threats to these systems and data is of particular interest to me in my role as the Federal Chief Information Officer (CIO). As CIO, I lead the OMB Office of E-Government & Information Technology (IT) (E-Gov), which is responsible for developing and overseeing the implementation of Federal IT policy. Even though my team has a variety of responsibilities, I will focus today's remarks on the Administration's response to increasing cybersecurity threats, and actions we are taking to improve the Government's background investigation process.

Governance of the Suitability and Security Clearance Processes

Beginning in 2008, the Suitability and Security Clearance Performance Accountability Council (PAC) was established through an Executive Order, comprised of the Office of Management and Budget (chair); the Director of National Intelligence (Security Executive Agent), the Director of the U.S. Office of Personnel Management (OPM) (Suitability Executive Agent), and the Departments of Defense (DOD), Treasury, Homeland Security, State, Justice, and Energy, the Federal Bureau of

Investigation, and other agencies. The inter-agency PAC oversees reforms to the processes that Federal agencies and the public rely on to ensure Federal employees, contractors or members of the armed forces are suitable for employment and can be trusted with access to facilities and sensitive information.

The PAC Security and Suitability Review

Last year, in light of increasing cybersecurity threats – including the compromise of information housed at OPM – the PAC initiated an accelerated inter-agency review of the Government's suitability and security clearance background investigation process. Its goals were to determine how to further secure the sensitive data collected as part of the background investigation process and to determine improvements that could be made to the way the Government conducts background investigations.

The review resulted in the announcement last month of a number of steps that the Administration is taking to improve the Government's background investigation process for Federal employees and contractors. I would like to highlight major actions we are taking with our partners in OPM, DOD, and ODNI as well as other PAC agencies.

The New Background Investigations Bureau

In order to create a more secure and effective infrastructure, the Administration will establish a new Federal entity, the National Background Investigations Bureau (NBIB), which will strengthen how the Federal Government performs background investigations. There are a number of organizational changes that will take time to implement but result in significant improvements over time:

- The head of NBIB will be Presidentially-appointed, unlike the current structure, where the head of FIS is a career employee of OPM.
- The head of NBIB will be a full member of the PAC, whereas currently OPM's Federal Investigative Services (FIS) is a subordinate component of OPM and is not an independent member of the PAC.
- While the NBIB will report to the OPM Director, it will also be accountable to the PAC and its customer agencies, and will receive policy direction from the Suitability and Security Executive Agents.
- NBIB will be headquartered in Washington D.C., rather than in Boyers, Pennsylvania, which will allow for enhanced coordination with its inter-agency partners.
- NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up and new IT systems are developed.
- Not only will a cadre of inter-agency personnel help stand up the NBIB, but NBIB will also leverage the expertise of inter-agency personnel and customer feedback as part of its ongoing management.
- NBIB will have several inter-agency working groups with its customer agencies designed to ensure there is regular feedback incorporated into operational decisions.

Leveraging DOD's Expertise

We recognize that creating a new investigations service provider does not, by itself, resolve the challenges we face in securing the investigative data and systems. Thus, in addition to the governance and organizational changes above, the Administration intends for NBIB's IT systems to be designed, built, secured, and operated by DOD, in accordance with NBIB requirements. This will leverage DOD's expertise in information technology and cybersecurity for processing background investigations and protecting against threats, will better protect the sensitive information used to effectively adjudicate investigations, and bring the fullest security resources to bear against increasingly sophisticated and evolving threats.

- This approach will leverage DOD's significant national security, IT, and cybersecurity expertise, incorporating security into the fundamental design of the systems, strengthening the security of the data environment, and providing robust privacy protections.
- To support this work, the President's Fiscal Year 2017 Budget includes $95 million within DOD's topline to that will be dedicated to the development of these IT capabilities.
- The PAC will also establish an inter-agency cybersecurity advisory group to provide advice and counsel on system development and threat mitigation.
- These efforts are consistent with OMB's direction to all Federal agencies to phase out the use of legacy IT systems where possible, and to begin using modern and emerging technology tools and capabilities to adequately secure mission functions, systems, and information.

Implementation

While these changes will take time to fully implement, the Administration has taken, and will continue to take, a series of actions to strengthen the background investigations process, including:

- In March, the Administration will have established a dedicated transition team headquartered in Washington D.C. to develop and implement a transition plan to: (1) stand-up the NBIB, (2) ensure that the transition timeline fully aligns with business needs, (3) transition the management of new investigation IT capabilities to DoD, (4) migrate the existing mission, functions, personnel, and support structure of OPM FIS to NBIB, and (5) provide continuity of service to FIS's customer agencies during the transition.
- By October 1, the Administration expects to establish the NBIB with the new governance and organizational structure described above, including absorption of FIS.
- By the end of 2016, we expect to begin delivering new, modern government-wide capabilities such as eApplication and eAdjudication that will greatly improve the effectiveness, efficiency, and security of key aspects of the background investigation process.
- By the end of 2016, the PAC and the Performance Improvement Council will also develop and implement outcome-based metrics that measure the effectiveness of the vetting processes.

Role of the Cybersecurity National Action Plan

More broadly, enhanced cybersecurity across all Federal Agencies will be strengthened by:

- Implementation of the Cybersecurity National Action Plan (CNAP), which builds on the security measures implemented in response to the 2015 cyber incidents (e.g., expanding strong

authentication; increasing scans; patching critical vulnerabilities; tightening privileged users policies and practices; identifying and securing high value assets; hiring a new senior OPM cyber and information technology advisor). The CNAP takes near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, and maintain public safety and economic and national security.

Summary

Over time, these actions will lead to tangible changes to the way we conduct background investigations for our trusted employees, military members and contractors. Indeed, these efforts – like other successful reforms in this important area – will span more than one Administration. We look forward to working with Congress to create a more secure, efficient, and effective Federal background investigations infrastructure. I thank the Committee for holding this hearing and I am pleased to answer any questions you may have.

Chairman CHAFFETZ. Thank you.

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

STATEMENT OF WILLIAM EVANINA

Mr. EVANINA. Thank you, sir. Chairman Chaffetz, Ranking Member Cummings, members of the committee, first, thanks for having the opportunity to have me representing the intelligence community be here with you as part of this panel and to take part in the formation of the National Background Investigations Bureau and provide an update on substantive reforms and security clearance processes that we have done so far in this effort.

As the national counterintelligence executive and the Director of the National Counterintelligence and Security Center, I have the privilege of working with some of the best and brightest security minds in the United States Government. I am honored to share with you the progress we have made with respect to security clearance reforms and raising awareness throughout the United States Government on the potential security threats resulting from multiple breaches and the theft of personally identifiable information known as PII.

The Director of National Intelligence is a principal member of the PAC, and I act on his behalf in this role. On behalf of the intelligence community, the ODNI strongly endorses this plan to create the National Background Investigations Bureau and leverage the Department of Defense's—all their skills, abilities, tools, and techniques to protect the associated systems and data. I am committed to this partnership with the NBIB and will continue our holistic and collective approach towards successfully implementing new security clearance processes.

In accordance with the Intelligence Reform and Terrorism Protection Act and Executive Order 13467, the security executive agent is responsible for directing the oversight of investigations and determinations of eligibility for access to classified information or to hold sensitive positions rendered by any executive branch department or agency.

These authorities also give the DNI responsibilities to develop uniform and consistent policies and procedures and to ensure the effective, efficient, and timely completion of investigations and adjudications.

We've been working diligently to establish a policy framework and infrastructure for robust engagement on national security processes across the U.S. Government. I have included examples of governance, policy, and standards in my statement for the record. However, I'd like to highlight just a few here today.

In October 2013, the DNI issued executive correspondence directing agencies to review and validate whether employees or contractors actually require eligibility for access to classified information. This effort resulted in a reduction of clearance-holders by approximately 18 percent across the United States Government. This effort continues today.

In June of 2015, the DNI issued correspondence on implementation of continuous evaluation, providing executive branch agencies direction in reevaluating clearance-holders on a more frequent and automated basis. And in June of 2015, OPM and ODNI issued their

first joint regulation on designating national security positions, which standardized this process across the entire government.

In my role as the national counterintelligence executive and the Director of NCSC, I have been emphasizing the benefits of merging counterintelligence and security because we know they are stronger together. This partnership provides the enhanced ability to both identify threats posed by foreign adversaries and at the same time enact security measures to mitigate those threats.

NCSC is actively reviewing and assessing all threats posed by foreign adversaries, including those related to cyber breaches and theft of PII. Specific to the theft of PII over the past few years NCSC initiated a comprehensive national counterintelligence and awareness campaign to educate those impacted, like members here in this panel, by the breach that happened last year, including former government employees and former contractors and their families.

This past September, my office began releasing educational awareness videos and materials for a Web site NCSC.gov and actively engaging with all departments and agencies on such topics as spear-phishing, social media deception, and human targeting. We are in the process of releasing a fourth video on travel awareness.

To date, the campaign has reached over 330 organizations to include over 100 U.S. Government departments and agencies, private sector groups, and cleared industry. I or my staff have participated in over 15 briefings and hearings to multiple committees to address CI and security implications of all breaches that have occurred in the last few years.

Additionally, NCSC has provided briefings to well over 150 Senate, House staff—and Senate staff to provide tools to mitigate such threat—threats for themselves, their families, their members, and constituents.

We continue to explore every possible avenue to maximize distribution of the campaign materials. We are currently partnering with the—with DHS and the White House using social media and private sector engagements. NCSC, leading the entire intelligent community, continues to provide enhanced awareness to individuals victimized by the recent breaches and provide mitigation strategies to thwart potential foreign adversaries.

In conclusion, NCSC values our robust partnership with OPM, OMB, and DOD and other PAC stakeholders in this committed endeavor. Together, we will continue to take our necessary steps to enhance government-wide policies and procedures in securing our systems and our data.

And once again, I would like to thank the committee for the opportunity to provide an update on security clearance reforms, formation of the NBIB, and NCSC's efforts to mitigate the impact of all the breaches, and specifically with respect to PII. We look forward to working with your committee and the rest of the Congress, and I'm happy to answer any questions you may have.

[Prepared statement of Mr. Evanina follows:]

Statement for the Record

Formation of the National Background Investigations Bureau and Security Clearance Reforms

William R. Evanina

Director of the National Counterintelligence and Security Center

February 25, 2016

Introduction

Chairman Chaffetz, Ranking Member Cummings, Members of the Committee, thank you for inviting me to be a part of today's hearing on the formation of the National Background Investigations Bureau, or NBIB, and provide an update on substantive reforms of the security clearance investigation process. As the National Counterintelligence Executive and the Director of the National Counterintelligence and Security Center (NCSC), I have the privilege of working with some of the best and brightest security minds in the United States Government (USG). I am honored to share with you the progress we have made with respect to security clearance reform and raising awareness throughout the USG on the potential security threats resulting from multiple breaches and theft of Personally Identifiable Information (PII).

The Director of National Intelligence (DNI) is a principal member of the Performance Accountability Council (PAC), and I act on behalf of the DNI at the PAC. In leadership with the Office of Personnel Management (OPM) (Suitability Executive Agent), the Office of Management and Budget (OMB), Department of Defense (DoD) and other stakeholder agencies via the PAC, I am committed to this partnership with the NBIB, and will continue our holistic and collective approach toward successfully implementing new security clearance business processes. Additionally, we intend to extend our collective successes on behalf of Security Clearance Reform activities across the policy, program development, and implementation landscape, government-wide.

DNI's Role as the Security Executive Agent (SecEA)

In accordance with the Intelligence Reform and Terrorism Prevention Act and Executive Order (EO) 13467, the SecEA, is responsible for directing the oversight of investigations and determinations of eligibility for access to classified information or to hold a sensitive position, rendered by any Executive Branch department or agency. These authorities also give the DNI responsibilities to develop uniform and consistent policies and procedures to ensure the effective, efficient and timely completion of investigations and adjudications relative to these national security determinations.

Security Clearance Reform Efforts

The NCSC, on behalf of the SecEA, has been taking an inter-agency and enterprise-wide approach to Security Clearance Reform across the Executive Branch. Many issues we collectively face require working closely with OPM, OMB, DoD, and stakeholder agencies consisting of expertise in credentialing, suitability and security processes.

We have been working diligently to establish a policy framework and infrastructure for robust engagement on national security processes.

Some examples include:

- December 2012: OPM and ODNI joint issuance of the Federal Investigative Standards aligning suitability and security investigations across government, including

implementing Continuous Evaluation (CE) and reducing the secret-level periodic reinvestigation from 10 years to 5 years.

- October 2013: DNI issued Executive Correspondence on Validation of Personnel with Eligibility for Access to Classified Information, directing agencies to review and validate whether each employee or contractor requires eligibility for access to classified information, resulting in a reduction of clearance holders by approximately 18% across government from FY13 to FY15.
- October 2013: DNI issued Executive Correspondence on Periodic Reinvestigations, directing agencies to reduce the number of out-of-scope Periodic Reinvestigations by using a risk-based approach and prioritizing submissions.
- July 2014: OPM and ODNI jointly issued the Implementing Plan for the National Training Standards, standardizing investigator and adjudicator training across the USG.
- December 2014: DNI issued Executive Correspondence, Security Clearance Reciprocity Reporting Requirement, which announces the required collection of security clearance reciprocity metrics required by the FY 2014 Intelligence Authorization Act.
- January 2015: OPM and ODNI jointly issued Executive Correspondence, Approval of the Quality Assessment Standards for Background Investigations, to provide executive branch agencies guidance in assessing the quality of background investigations.
- June 2015: DNI issued Executive Correspondence, Implementation of CE, which provides executive branch agencies direction on the implementation of CE to support the more frequent vetting of personnel eligible for access to classified information or to hold a sensitive position.
- June 2015: OPM and ODNI issued their first joint regulation - 5 CFR 1400, Designation of National Security Positions which provides clarifying guidance to agencies on designating national security positions, standardizing processes across government.

Going forward, the ODNI, OPM, OMB and DoD will continue to provide active leadership in monitoring performance and identifying and driving continual improvements. These priorities include improving access to relevant information, especially state and local law enforcement records; implementing CE across the executive branch; improving risk management approaches to reduce vulnerabilities in our current processes, including reduction of the total number of clearance holders and the backlog of periodic reinvestigations; and improving enterprise operations, to include strengthening oversight and government-wide implementation efforts while effectively managing limited resources.

Counterintelligence & Security

The integration of CI & Security within NCSC enhances our capability to fulfill our responsibilities to protect national security information. Counterintelligence provides an in-depth analysis of potential foreign intelligence entity exploitation of data gained during multiple data theft incidents inclusive of PII. In response to this analysis, Security policies and procedures to mitigate or uncover vulnerabilities which may be leveraged to exploit personnel with access to sensitive information.

NCSC is actively reviewing all threats, including those related to data theft. Specific to the theft of PII over the past few years, NCSC initiated a comprehensive national counterintelligence

awareness campaign to educate those impacted by the breach, including current and former federal government employees and contractors on threats associated with the breach and to help them mitigate tactics foreign intelligence entities may use in exploiting their compromised PII. In September 2015, NCSC began releasing educational and awareness videos and materials via NCSC.gov, and actively reaching out to departments and agencies, covering such topics as Spear-phishing, Social Media Deception, and Human Targeting; and expects to release a fourth and final video on Travel Awareness in the month of March.

NCSC, leading the Intelligence Community, continues to provide enhanced awareness to individuals victimized via the breach and provide mitigation strategies to combat potential exploitation by foreign adversaries.

To date, the campaign has reached over 330 organizations to include: over 100 USG departments and agencies, private sector groups, and cleared industry. In addition to these groups, NCSC has provided briefings to well over 150 Senate and House staff on how to mitigate threats for themselves, their families, their members and constituents. Additionally, I or my staff have participated in over 15 briefings and hearings to multiple committees to address the CI and Security implications with respect to the theft of the PII.

We continue to explore every possible avenue for distribution of campaign materials, including partnering with DHS and the White House, press releases, social media, conferences, and numerous private sector speaking engagements.

Conclusion

NCSC, representing the entire Intelligence Community, remains committed to working with Congress to address any issues or concerns regarding the aftermath of the breach.

NCSC values our partnerships with OPM, OMB, DoD and the other PAC stakeholder agencies, and together, we will continue to take the necessary steps to enhance government-wide policies and procedures, and securing systems in the clearance process.

Once again, I would like to thank the Committee for the opportunity to provide an update on substantive reforms of the security clearance investigation process and to discuss our response to last year's OPM breach. We look forward to working with your Committee and the rest of Congress in the future on this process and I am happy to answer any questions you may have.

Chairman CHAFFETZ. Thank you. I now recognize myself for 5 minutes.

Ms. Cobert, we have some outstanding document requests. When will we get those?

Ms. COBERT. We're continuing ——

Chairman CHAFFETZ. Microphone, please.

Ms. COBERT. I will get this right. I apologize.

We are continuing to work through those. I know we made a delivery of a significant number of documents by the date of the subpoena, and we are working with your office to prioritize those. We are working to get them to you as fast as we can.

Chairman CHAFFETZ. And I would hope that the ranking member would also join us in those document requests.

Mr. CUMMINGS. I will.

Chairman CHAFFETZ. Thank you. I want to talk about social media. Ms. Cobert, will all agencies look at social media for those applying for security clearances?

Ms. COBERT. Thank you, Congressman. Let me start and I think ——

Chairman CHAFFETZ. We don't have much time.

Ms. COBERT. We are in the process working with the DNI ——

Chairman CHAFFETZ. Why wouldn't you look at social media?

Ms. COBERT. In looking at social media, we want to make sure that we are looking at it in a way that is effective, that brings insight to the process, that reflects what's in that information and it's done in an appropriate and systematic way.

Chairman CHAFFETZ. Will ——

Ms. COBERT. And that's the new policies that we are working to put in place.

Chairman CHAFFETZ. Will you require that each person applying for a security clearance provide their online identities to you?

Ms. COBERT. The specifics of the social media policy are ones we are working through with the DNI. As the security executive agent, they set the policies that we follow.

Chairman CHAFFETZ. Okay. Mr. Evanina, why the hesitation on providing social media information?

Mr. EVANINA. Sir, there is no hesitation. We've been working robustly the last few years with the Department of Defense to enact I think what we believe to be a robust policy on selecting ——

Chairman CHAFFETZ. So what is the policy in short?

Mr. EVANINA. Well, the policy in short is utilization of social media to enact investigations and adjudications of individuals who request a security clearance. And that's in the process as we speak.

Chairman CHAFFETZ. Do you require anybody seeking a security clearance to provide their online identities?

Mr. EVANINA. Well, not at this point right now, but through the pilots we have issued throughout the government and DOD, we ——

Chairman CHAFFETZ. See, this is my frustration. You have been working on this for years, and you haven't yet implemented a policy that requires them to identify their online identities. How hard is that? It is a one-sentence question.

Mr. EVANINA. Well, I think the difficulty begins when you have the mixture of executive branch organizations, and currently right now the issues are multifaceted. It involves the utilization of privacy issues for the ——

Chairman CHAFFETZ. What privacy issue do you have? By its very definition, social media means you are not being private.

Mr. EVANINA. I concur, sir, but the issue is getting past the password and having authority granted or waiver to get through the password to get to the information which is in the social media.

Chairman CHAFFETZ. So we are going to grant them a security clearance to access the information of the United States of America, information that can't be shared to the public, and they won't share their information with you?

Mr. EVANINA. I hope not.

Chairman CHAFFETZ. Well, when are you going to have this policy done?

Mr. EVANINA. Well, the policy is currently out of the ODNI, and it is in coordination with the executive brach of the government.

Chairman CHAFFETZ. When is it going to be done? Who is in charge of this?

Mr. EVANINA. Currently ——

Chairman CHAFFETZ. Who do we call to this committee to explain this to us?

Mr. EVANINA. It's currently with the Office of Management and Budget for coordination.

Chairman CHAFFETZ. Okay. Mr. Scott, where are we at with this?

Mr. SCOTT. I don't know, but I will find out and get back to you.

Chairman CHAFFETZ. And you are the—I need to get it right—chief information officer for the—so—I am sorry. The chief information officer for the United States of America.

Mr. SCOTT. I just don't know today where we're at on that particular policy ——

Chairman CHAFFETZ. This is the cluster ——

Mr. SCOTT.—but I will find out and get back to you.

Chairman CHAFFETZ. This is the cluster that is the Federal Government. This should be such a simple question. It should be on your form, show us all your online identities. And then as we are doing a background investigation, how can you not go look at their Facebook page or their Twitter posts or their Instagram or Snapchat or any of the other ones? We don't do that? How moronic are we? I mean, come on. My 14-year-old could figure this out. What is the hesitation?

Yes, this is the problem. It is just silent. I was planning to take 20 seconds on this question and we should probably do an entire hearing on how we don't look at the social media of people we—we give top security clearance, we are showing people—we are putting people's lives in danger, their very—and we can't go online and look at their social media? All right. I have got to keep going but this is—go hire a bunch of teenagers. They would do it better than we are doing it. I mean, they know how to do this stuff but we don't as a government—ISIS has figured it out. They know how to do it, but we don't seem to do it.

All right. With the National Background Investigation Bureau, which inspector general has jurisdiction, Mr. Halvorsen?

Mr. HALVORSEN. I don't think a single inspector general will have jurisdiction. I can assure you that certainly the DOD IG, as we build the IT systems, will look at this. I ——

Chairman CHAFFETZ. Will you provide access? Will there be any limitations on access for the inspector general for OPM to look at this?

Mr. HALVORSEN. No, sir. We couldn't do that legally. They have access legally to look at all that, as does the General Accounting Office, and I am sure there will be many committees and offices that will want to have access to this. Legally, they'll be entitled to that, and we will give it to them.

Chairman CHAFFETZ. I appreciate it.

As the DOD's CIO, are you ultimately going to be responsible for the IT system at the NBIB?

Mr. HALVORSEN. Yes.

Chairman CHAFFETZ. And will you report to the Director of the NBIB or will you be able to make IT decisions and overrule the NBIB? Who is in charge?

Mr. HALVORSEN. In the end, DOD is in charge of the technical decisions, but I will stress we have worked well together with all of the members of this panel. We will continue to coordinate with all of the customers. We will continue to do this in a cooperative way. But in the end, I report to the Secretary of Defense. The Secretary of Defense is the biggest customer of the NBIB, and I assure you, I don't expect any problems to come up. If they do, I'll take them directly to the Secretary of Defense.

Chairman CHAFFETZ. But you are in charge, correct?

Mr. HALVORSEN. I am the accountable official for building this IT system the right way.

Chairman CHAFFETZ. I appreciate it. My time is expired. I will now recognize the gentleman from Maryland, Mr. Cummings.

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

James Clapper, Director Cobert, the Director of National Intelligence, recently told an audience at the Naval Academy that the number one threat facing our country is cyber attacks. He said, "The cyber threat is here. It is upon us now and we need the people here today to help us defend our systems and our nation."

I do appreciate the collaborative interagency approach you all are taking with regard to this proposal. I would like to know what you are doing to enhance oversight of government contractors because our investigations have shown that contractors have repeatedly been the weak link in Federal cybersecurity. In the OPM data breach, for instance, cyber attackers first breached KeyPoint and then disguised themselves as KeyPoint employees to gain access to OPM's background investigation system.

Director, what steps are you taking to require KeyPoint and other contractors to shore up their IT security?

Ms. COBERT. Thank you, Congressman. Improving our ability to work with our contractors on cybersecurity is a key priority for us at OPM, and I know it is across the executive branch. We have been reviewing the clauses in our contracts and working to ensure

that we can make—that those have the provisions that we need going forward.

There's an effort underway with NIST, with the Office of Federal Procurement Policy to develop standards. One specific example, we are re-competing the field investigation contract this year, the contract under which CACI and KeyPoint do that work today. That contract will be re-competed.

As we're preparing to re-compete that contract, we have been working actively to include those clauses. We've in fact already been working with the Department of Defense to look at the kind of clauses we're going to put in place in that contract to make sure that we can leverage their expertise here as well. So we take this seriously. We're reviewing the contracts, and that's just one example of how we're moving that forward.

Mr. CUMMINGS. I am going to come back to those clauses in a minute. But, Mr. Scott, what measures is the administration taking to prevent the misuse of Federal contract IT systems to penetrate government IT systems?

Mr. SCOTT. Part of our updated guidance that's coming out, Ranking Member Cummings, includes standardized contract language that we expect will be adopted in all the contracts that agencies use for IT. And that's a way of getting consistency and then also being able to measure performance against that.

Mr. CUMMINGS. Well, as you know, another OPM contractor, Anthem, was also breached, and the personnel information of nearly 80 million Americans was compromised, including names of Federal employees. Experts believe these were all part of a sophisticated, coordinated cyber espionage campaign. They all occurred at about the same time, they all targeted sensitive information about Federal employees, and they all were carried out using similar malware.

Mr. Halvorsen, does it worry you that our adversaries can target private corporations with relationship to the Federal Government to obtain sensitive information about Federal employees? And how does the administration's proposal improve cybersecurity at Anthem or other government contractors?

Mr. HALVORSEN. Well, it certainly worries me that organizations can and governments can target U.S. companies. I think what the administration has done here, by allowing DOD to be part of this, we have in DOD already some existing clauses and regulations that require our contracts to highlight cybersecurity.

I think everybody at this table, Mr. Scott has certainly been leading an effort to improve Federal cybersecurity everywhere, taking those clauses. We partner a lot. Ms. Cobert, as the acting OPM Director, has been doing the same thing. So I think we're handling the threat and moving forward in all the right directions to put in the right clauses, the right rules, the right things.

We're also at DOD working with Mr. Scott expanding the communications we have with private contractors so that they can do better security on their own and feeding them better intelligence about what the threat is.

Mr. CUMMINGS. After the attack, Anthem did not ask the incident response team at US–CERT to investigate. You would think that Anthem as a government contractor would be required—and

this goes back to these clauses, Director Cobert—would be required to allow a government forensics team in to investigate the theft of government employees' personal information.

Director Cobert, why wasn't Anthem under any contractual requirement to report breaches involving government data to US–CERT? Why is that?

Ms. COBERT. Congressman, Anthem was under requirement to report breaches to OPM to our situation room, and we can then work with them on how to respond. I was not there at the time so I don't know the specifics of that. I know we are having an ongoing set of discussion with Anthem and our other health insurance partners about how to strengthen cybersecurity and how we're going to work with them going forward ——

Mr. CUMMINGS. So that is a ——

Ms. COBERT.—including that possibility.

Mr. CUMMINGS. That is a part of the contract now, though? In other words, the contracts—I take it was in the contract before. They didn't do it. Is that what you are trying to tell me?

Ms. COBERT. No. To the best of my understanding, the obligation in the contract is to report to OPM.

Mr. CUMMINGS. Okay.

Ms. COBERT. That they did do.

Mr. CUMMINGS. Okay. Now, what about US–CERT?

Ms. COBERT. I don't believe that the contract requires them to report to US–CERT, but as we're looking at the new contracts and as we're working with all of our health insurance partners, that is one of the options we are exploring.

Mr. CUMMINGS. Would you get back to us on that because, as I said before, this is a, you know, weak link that I think we don't want to miss, particularly when you all are putting things together and trying to tighten up any kind of loopholes. That is something that I would hope that you all would take a look at and get back to us on.

I yield back.

Ms. COBERT. I will do that.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from Oklahoma. I appreciate his leadership on this issue, along with Mr. Lieu. But I will now recognize Mr. Russell of Oklahoma for 5 minutes.

Mr. RUSSELL. Thank you, Mr. Chairman. And I do thank the panel for being here today and for making every attempt to resolve this situation. However, we have got some problems here.

Mr. Scott, who is currently funding the FIS?

Mr. SCOTT. I believe that's part of the revolving fund in OPM. Beth could probably answer that ——

Mr. RUSSELL. Okay. And I am getting a nod from Ms. Cobert there. So it currently comes out of OPM, and yet, as I heard it stated by you that this will come—this $95 million to stand up the Bureau will now come from top line of Department of Defense. Why is it that Department of Defense has to pay for it?

Mr. SCOTT. This would be added to the DOD budget and give them the funds needed to develop the systems.

Mr. RUSSELL. Will it come out of OPM's budget.

Mr. SCOTT. I don't ——

Mr. RUSSELL. Yes.

Mr. SCOTT. Since the ——

Mr. RUSSELL. Therein lies the problem.

Mr. SCOTT. Since the fiscal year 2017 budget isn't the reality yet, I don't know the answer to that.

Mr. RUSSELL. Well, I think we know in principle that if FIS was funded by, you know, OPM, then it just makes good sense that the monies would be transferred.

Ms. Cobert, would you like to answer that?

Ms. COBERT. The Federal Investigative Service operates with a revolving fund. It—the agencies that use those services pay fees for those services. That is the core of FIS's funding is through the fees that agencies that require background investigations pay for those services. So the funds come from agencies through interagency agreements into OPM. It's a revolving fund, not appropriated funds.

Mr. RUSSELL. Okay. Well, and that helps somewhat, but here is the problem. And while I agree that DOD is the biggest user, herein lies the overarching problem. We have allowed, out of a necessity of cost saving, of elimination of backlogs that we got into this situation where 18 million records have been breached. Whatever it was we hoped to gain has absolutely materially aided our enemies for probably two or more generations. They will be able to mine incredible data. It does not take a genius to figure that out. And so now, as we are getting ready to set up potentially another house, we want to make sure it is not a house of cards.

I have real concerns that this money is coming out of Department of Defense specifically, and here is why. For $95 million you could have 60,600 soldiers being paid, and we are talking about additional cuts. And so now because we have had a breach and now we are going to try to make a bureau, we are going to cut 30,000 soldiers from the Army and further diminish the Marine Corps. I mean, this is the problem. We are weakening our country. We are weakening the Department of Defense. We are weakening whoever might have a security clearance.

I don't think that the solution is take it out of top line of Department of Defense, and I will take real issue with that.

I also sit on the House Armed Services Committee, and with my background, I am given a little bit of respect and wide berth on those issues. So I am not satisfied with those answers.

Here is another one: responsibility. Okay. And I appreciate, Mr. Halvorsen, all that you do. I do understand it. And you were careful to accurately describe the authority pieces. You said that DOD would be technically in charge, that DOD will be allowed to be a part of this. And I think that is accurate language, but therein again lies the problem. When you are in conflict with your recommendations, will you have the final authority to push that through for national security?

Mr. HALVORSEN. Sir, I believe that I will, and I ——

Mr. RUSSELL. Believe?

Mr. HALVORSEN. Yes, sir. And I'll stress again ——

Mr. RUSSELL. But the wiring diagram could conflict with that, does it not, because now Department of Defense is going to have to go through, you know, the Bureau, who goes through OPM, and

then we will talk about it on the PAC. You may not have that authority, is that correct?

Mr. HALVORSEN. Sir, I don't think that is correct, and I would say this. The wiring diagram isn't finished. But I will tell you this. Again, I report to the Secretary of Defense. Secretary of Defense has made it very clear to me ——

Mr. RUSSELL. Oh, I am sure he has.

Mr. HALVORSEN.—number one customer. I ——

Mr. RUSSELL. But if OPM disagrees with the Secretary of Defense, then we have got a problem, do we not?

Mr. HALVORSEN. If we had that problem, I think we might have a short problem. I don't think in the end OPM is going to tell the Secretary of Defense ——

Mr. RUSSELL. But the wiring diagram ——

Mr. HALVORSEN.—not to build it.

Mr. RUSSELL.—is set up potentially for that type of flaw, and this is a problem. One thing I did learn as a soldier—maybe it doesn't happen here in Congress but it certainly did on a battlefield—you have to have unity of effort, and not just unity of effort. You have got to have somebody clearly in charge.

And here is my big beef. If the Department of Defense is going to clearly have the greatest level of responsibility to protect these documents, then they by golly better have the authority to make it good, and we ought not to be weakening and diminishing our land forces to pay for some data breach. Those monies, we have got to figure out a different way.

And with that, Mr. Chairman, I have exceeded my time. Thank you for your indulgence.

Chairman CHAFFETZ. I thank the gentleman. I will recognize the gentlewoman from the District of Columbia, Ms. Norton, for 5 minutes.

Ms. NORTON. Thank you very much, Mr. Chairman.

Director Cobert, the breach that has occurred into Federal employee data is deep indeed. In fact, I would guess that if you worked for a private corporation, much of that data would not be even in the hands of your employer, for example, your spouse's data, your children's data, the kind of data that is appropriate for a government agency, and yet minimally in the beginning only 18 months and $1 million was allowed in protection. I am grateful to the appropriators it is going up to 10 years and $5 million. I have a bill for lifetime protection.

Isn't it true that much of this information, information not only regarding the employee but the employee's family, spouses, children, is unchangeable, cannot be somehow mitigated by making changes in the particular data that the hackers have?

Ms. COBERT. Yes, that is correct, Congresswoman.

Ms. NORTON. To your knowledge, has any use been made of this data to this point?

Ms. COBERT. Congresswoman, we are in continual dialogue with our partners in law enforcement and the intelligence community, and we have not seen misuse of this data.

Ms. NORTON. This is what is so worrisome, that the hackers—I don't know if they are simply mischievous or if they are holding the data until it is useful. But I want to say again that I don't see how

OPM can do anything but recommend to the President that there be lifetime protection.

Look, this protection may never be used. That is to say it may never cost the government much. It is like an insurance policy. So I must say that the very least we owe Federal employees, given this breach, it would seem to me is lifetime protection for data that cannot be changed.

I appreciate—and do you have any real way to monitor whether or not any use is being made of this data?

Ms. COBERT. Congresswoman, there's—we are, as I said, in dialogue with the FBI, with the NCSC, the DNI, and others ——

Ms. NORTON. What obligation ——

Ms. COBERT.—to monitor those ——

Ms. NORTON. What obligation would you be under to inform an employee were you to find that use has been made? How would that work?

Ms. COBERT. We would work with those bureaus to understand the right way to inform them. We've also continued to remind ——

Ms. NORTON. There is no protocol yet for what to do?

Ms. COBERT. We haven't had—we continue to remind employees about the opportunity to sign up for the monitoring services. The levels of penetration of people signing up for those services far exceeds what we've seen in the private sector context. We'll continue

——

Ms. NORTON. No, but see, that is not my question.

Ms. COBERT.—to work with them.

Ms. NORTON. My question is you discover that some use has been made. What do you then do?

Ms. COBERT. It will—we were—that's why we need to work with law enforcement. We need to understand the nature of how that data is being used ——

Ms. NORTON. Ms. Cobert, I hope ——

Ms. COBERT.—to take the appropriate actions.

Ms. NORTON.—during your—I don't have much time. I hope during your time that an actual protocol is set up for immediate notification in some way that the employee can be further protected.

Look, I am interested in the fact that 60 percent of the investigations are done by contractors. I understand perhaps the reason why, but I noted that one of the contractors Anthem, which is not discussed as much, had jurisdiction over health insurance of Federal employees, and 80 million Americans' information or 80 million Americans was breached.

And of course that is very, very personal information, but they declined to let US–CERT investigate the breach. I can't understand that. These people are acting in the place of the government. Shouldn't the people who provide these services, have the sensitive information, be required to institute equivalent security measures, including having somewhat equivalent to the government or the government come in to investigate a breach?

Ms. COBERT. Congresswoman, we are working with our health insurance partners like Anthem on how to enhance their cybersecurity and our visibility into that. We are working on that

——

Ms. NORTON. Why wasn't US–CERT ——

Ms. COBERT.—with our inspector general.

Ms. NORTON. I mean, these people work for the government. Why wasn't US–CERT allowed to investigate a breach of Federal employee data? Why isn't that routine?

Ms. COBERT. Congresswoman, those are the—well, the kinds of clauses we were looking to implement going forward. The Anthem incident and the Anthem contract predated my time at OPM, but I know the health and insurance part of OPM, with our senior cybersecurity advisor Clif Triplett is working and in discussion with those insurers ——

Ms. NORTON. So you believe ——

Ms. COBERT.—how to do ——

Ms. NORTON. You believe that there should be an investigation by the government or by an independent auditor when there is a breach by one of these contractors. Is that the case?

Ms. COBERT. I believe that we need to bring the best resources we can to bear on these situations, and we need to put in place clear processes that reflect the challenges that we face today, and that's what we're working to do.

Ms. NORTON. Mr. Chairman, I wish we could get an answer to that question. I understand she's new, but if a contractor cannot be investigated in the same way that, for example, the IG will investigate a similar breach of a Federal agency, then I think we have a problem. I think we ought to give her time, but I think that question needs to be answered one way or the other with respect to contractors.

Chairman CHAFFETZ. I concur. I think this—if they are going to be allowed and are given access, whether they are a contractor or employee, the IG ought to be able to investigate it and not just create this fictitious firewall and say, oh, you can't look over here. We saw this at the Department of Education. They have 184 databases and yet nobody is looking at them.

And so I would agree. And I think this is a good bipartisan thing that we can push. We have brought this up previously with Ms. Cobert, and you can see the frustration that we see. We need an actual solution to this problem and challenge. I know you are new, but we need that.

And I also want to follow up with Mr. Russell here. We as a Federal Government have spent $525 billion plus over the last 7 years, and our IT doesn't work. And that is a tremendous frustration to go have to grab money away from our troops to clean up a problem that should have never been there in the first place, again part of the frustration.

And I do hope in this similar vein we can work in a bipartisan way to understand where the funding component comes and that this be of the utmost priority. But to grab it out of the troops' budget is probably the last place we should do that. So I don't know if you wanted to add anything to that. Sure.

Mr. CUMMINGS. You know, as I am listening to you, Mr. Chairman—and I guess this would be for you, Mr. Scott; I am not sure—is it that the IT system is so huge that we can't get it together? Do you follow what I am saying? Is it too big to improve? Do you follow me?

Mr. SCOTT. Yes, well, let me talk about the case generally across the Federal Government. And we've heard from every CIO that getting the funding to go replace any of these large systems has not been something they've been able to do in their normal budgeting process. It's why we put together the ——

Chairman CHAFFETZ. But wait, wait, wait, wait ——

Mr. SCOTT.—Cyber National Action Plan.

Chairman CHAFFETZ.—wait a second. Wait a sec. Wait a sec. You are getting more than $80 billion a year, and that isn't enough?

Mr. SCOTT. No. There's a lot of money, but the easiest money to get is money to sustain the old legacy systems that get more expensive every year because of lack of skills on old COBOL systems. The security that you put around those is more costly. And the hardest money to get is money to go develop new ones. It's why we've proposed the IT Modernization Fund that would give agencies access to the capital they need to go replace these things, and it's a core part of the CNAP plan that we've put together.

Chairman CHAFFETZ. Well, I have got to recognize the gentleman from Florida, but I think that is hogwash. You asked for about $3 billion, and yet you have had $525 billion over the last 7 years. To suggest we are just $3 billion away from actually solving this problem is ridiculous. And you spending 70 percent of the budget on the legacy systems, only 30 percent investing in new systems, and even the procurement ——

Mr. SCOTT. It's worse than that.

Chairman CHAFFETZ. Yes. And there is a talent portion to all that, but I don't think it has been a lack of funding, $80 billion a year. This is not a funding issue. One good trip to Best Buy and you could do better than we are doing now. That is the concern.

So let me recognize the gentleman from Florida, Mr. Mica ——

Mr. CONNOLLY. Mr. Chairman?

Chairman CHAFFETZ.—for 5 minutes.

Mr. CONNOLLY. Mr. Chairman?

Chairman CHAFFETZ. Yes?

Mr. CONNOLLY. If the gentleman from Florida would just withhold for one second, I share the chairman's concern, and I would simply suggest to him that one of the things I think we need to do—because the statistic gets bandied about we are spending 70 or 80 percent maintaining legacy systems. I think our committee ought to drill down on that, and I think one way we do that—and Mr. Scott can help us here—let's actually get an inventory agency by agency of what we are talking about so we have a better handle on that. And it would allow us then in some depth to work with agencies about, well, what would it take to replace these things?

Chairman CHAFFETZ. And I ——

Mr. CONNOLLY. Why are they costing so much money?

Chairman CHAFFETZ. And I would agree with that. One of the reasons I called for the dismissal of Ms. Seymour is for years the inspector general had been asking for an inventory. The Office of Personnel Management went for years, didn't even know how many laptops and how many ports. I mean, how can you solve the problem if you don't even know what the inventory is?

Mr. CONNOLLY. Yes.

Chairman CHAFFETZ. And so I totally agree with the gentleman from Virginia. This is part of the problem. This is why you have—when you have years of an inspector general saying it is better to unplug the system than to continue on, we have to heed those.

Mr. CONNOLLY. I thank my friend from Florida for his courtesy and I thank the chair.

Chairman CHAFFETZ. I will now recognize the gentleman from Florida, Mr. Mica. Thank you for your patience.

Mr. MICA. Thank you, Mr. Chairman.

I had the opportunity—and I still don't like Newt Gingrich for what he did to me, but made me chairman of the Subcommittee on Civil Service for 4 years, and I thought we had problems then. And actually, those were our glory days. I think we have reached the absolute bottom of the pit. I wish you well, Ms. Cobert. It is just unbelievable. I was just thinking of the money we have spent. I worked with the gentleman from Virginia on consolidation of IT systems. I think we did, Gerry, a hearing. Are you all still doing your retirement processing for Federal employees by hand?

Ms. COBERT. We are working to ——

Mr. MICA. Are you doing them by hand?

Ms. COBERT. Some more elements of it are digital ——

Mr. MICA. That was after spending ——

Ms. COBERT.—but much of it is manual still.

Mr. MICA. It is manual. Gerry, they spent a quarter of a billion dollars setting that up, and then now they are still doing it by hand. That is not what this hearing is about, but you take it whether it is—this is about security clearance reform. My God, they are putting in this system, which is at the expense of DOD, and it is going to be in place when? Can somebody tell me? You are doing the IT part of it? October? When? Hello?

Mr. HALVORSEN. The system will start being built in '17, and hopefully, by the end ——

Mr. MICA. So it is not until '17?

Mr. HALVORSEN. Yes, sir.

Mr. MICA. Okay. What is the backlog now? You have 388,000 new background investigations pending? Is that right, Ms. Cobert? And I have 117 periodic reinvestigations backlogged, half a million ——

Ms. COBERT. We are ——

Mr. MICA.—and the IT system is going to be in place in '17?

Ms. COBERT. Congressman, the ——

Mr. MICA. Well, is the backlog—I mean, that is what staff is giving me. I am only told ——

Ms. COBERT. You know, the figures I have on the backlog, we think about the backlog in terms of the timeliness for doing those ——

Mr. MICA. It is a half ——

Ms. COBERT.—investigations ——

Mr. MICA. It is a half ——

Ms. COBERT.—so yes.

Mr. MICA. It is a half a million backlogs right now. We don't have a system in place. I really even don't know where to start. If I was doing something, I would probably look at putting some—there are plenty of people that can conduct these investigations.

There are companies that do that. Can you contract with some of those folks? Can we get this in bite-size? You can only eat an elephant a bite at a time, I am told.

Ms. COBERT. So, Congressman, we have systems that support background investigations today. We have made strides over the last months ——

Mr. MICA. But you are going to ——

Ms. COBERT.—in making those more secure, and then we are going to rebuild them ——

Mr. MICA. They are building ——

Ms. COBERT.—with security.

Mr. MICA.—you this system, and then you are going to run it?

Ms. COBERT. No, DOD will operate the new systems.

Mr. MICA. But ——

Ms. COBERT. We are currently running the existing systems.

Mr. MICA. And who is going to conduct the investigations?

Ms. COBERT. The investigations will be ——

Mr. MICA. By this new agency?

Ms. COBERT. Will be conducted by the National Background Investigations Bureau.

Mr. MICA. Oh, folks, hang on to your shorts on this one. By the time you get the IT in place and the money you are going to spend, and then by the time you get OPM up and running, I mean, you can't even get the personnel to do the manual processing of the retirement. I think we are headed for another disaster. God bless you, but I am telling you, you have got to take this a bite at a time. You need to get contracts out. You need to get it out of OPM. Building this system, it is designed to fail. We will be back here the next Congress in '17. I guaran-damn-tee you—and put that in the record, it is a new word—that this will continue to be a disaster the way it sounds like you are putting it together.

I haven't even gotten into the issue of our personal records being hacked. Where are we on that? I mean, I got a notice that mine were hacked. Have you taken protections for all of us? I don't know if I signed up for whatever you offered, but we have millions of records hacked in OPM. What is the status of that?

Ms. COBERT. We have, working with the DOD, been through a process to notify individuals ——

Mr. MICA. I have been notified.

Ms. COBERT.—whose records ——

Mr. MICA. What is the remedy? I mean ——

Ms. COBERT. So there is services available ——

Mr. MICA. Yes, I just started getting—this week, I started getting scam calls from different groups that I have never gotten before at home. Member of Congress, what is the status of protecting me? Okay. Let's not even do me, but we have got hundreds of thousands of Federal employees out there.

Ms. COBERT. So we have provided these services. We have notified individuals and repeated that they had the opportunity to enroll ——

Mr. MICA. So we have to sign up. You have taken nothing preemptive to help us.

Ms. COBERT. We—these services are in place for you to receive ——

Mr. MICA. Okay.

Ms. COBERT.—the monitoring services. You have to provide your personally identifiable information, and we cannot legally ——

Mr. MICA. I don't trust ——

Ms. COBERT.—do that on your behalf.

Mr. MICA.—giving you any more of my information. It has already been hacked and people have it. I just want to know what we are doing preemptively to help people who have been hacked who have worked for the Federal Government or are working for the Federal Government.

Ms. COBERT. We have provided them services. We have ——

Mr. MICA. That is ——

Ms. COBERT.—provided them information about how they can protect themselves ——

Mr. MICA. Well, I think if you ——

Ms. COBERT.—and we are working with them to the extent they have an issue ——

Mr. MICA. If you could come back ——

Ms. COBERT.—to help restore their identity ——

Mr. MICA. Come back with another plan ——

Ms. COBERT. Restore their identity.

Mr. MICA.—and look at what I suggested. Thank you, Mr. Chairman. I yield back, and I will be back.

Chairman CHAFFETZ. Thank you. I now recognize the gentleman from Massachusetts, Mr. Lynch, for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. I want to thank the panelists for helping the committee with its work.

The standard form 86, very, very extensive and very thorough, and it goes into a person's entire history, their family, very, very in-depth investigation. That is what was hacked in many cases with respect to the hacks against OPM. And when Ms. Archuleta and Ms. Seymour were here last time, I asked them point blank if any of that information was encrypted. And the answer was no, we gathered all of this information at OPM, put it in one repository, and then did not encrypt it. So we basically invited people to come in and hack and basically get all the information. There were no firewalls or anything like that. So it was just colossally bad, bad management.

Now, I support the move to DOD because you have got at least some record of protecting information. It is in the vital interest of this country to do so. Are we going to be able to move that information over and secure it? I know a lot of it has already been hacked, but what is the next step on that, Mr. Halvorsen?

Mr. HALVORSEN. Yes, sir. We will move the information over. We will use the proper levels of encryption on all the levels of the data and have a leveled and layered defense of all of that data, and it will be physically and virtually inside the DOD boundaries.

Mr. LYNCH. Okay. And so there are about 4 million Americans that have to have security clearance. That is both Federal employees and contractors. And there is about 600,000 a year that we are issuing new clearances to. I would like to think that the idea that by October of 2017—is that what we are talking about when the system is going to be up and running or is it '16?

Mr. HALVORSEN. We will have the system begin running, yes, October of '16. It will not be completed by October of '16, but we will begin to execute new parts of that system in October of '16. It will take the following year to complete that given the complexity of the system.

Mr. LYNCH. I just think that that is happy talk with all due respect. With the problems we are having with pensions and—you know, I used to chair the Subcommittee on Federal Employees, and, you know, we have had longstanding problems with that. I just think that is, like I say, happy talk. That is just dream world stuff. We have had terrible, terrible problems with just getting basic information up and running. We are still doing stuff manually, as the gentleman from Florida pointed out.

But interestingly enough, the only stuff that hasn't been hacked is the stuff that we are doing by hand. And I am sure that is not intentional, but that just demonstrates the weakness of our system.

Let me ask you, is there any value, you know, because if someone is going through this, you know, top secret clearance process, that is an important role. And if they are looking for that type of clearance, we have a concomitant duty, I think, to make sure that person is thoroughly, thoroughly vetted. And I agree with that.

But is it necessary to have all those folks online and to have the ability of one person sit down and get access to all of them? Or is there an opportunity to have some type of firewall, Ms. Cobert?

Ms. COBERT. Congressman, we have taken steps already to move in the direction you are describing. We have put in place more advanced firewalls. We have increased the segmentation of the data. We have improved encryption. We are not finished, but we are working towards that.

And as we think about the redesign of the system—I'm sure Terry could talk more about it—the question you're posing about who needs to have access to what elements of the data, how do we store it effectively, how do we allow people what they need from a business operation perspective to interact with the data but have it in a much more segmented way is part of the future design.

We've put in remedial measures on the current systems. We have much better firewalls. We have much more stringent criterias for access to that data, so we've done the things that we need to do within the existing systems, but we fundamentally need to build them with security by design built in, and that is what our partners from DOD are going to help us do.

Mr. LYNCH. Okay. One last point. The recently passed omnibus bill that the President signed says that "in relevant part the enhanced personnel security program of an agency shall integrate social media." So shall means shall. And so all this hedging is contrary to congressional intent.

Ms. COBERT. Congressman, we are actively working to do that today on the SF–86. It requires folks to put their email address and aliases. We are working closely with the DNI to put that in place.

Mr. LYNCH. Okay.

Ms. COBERT. The pilots that DOD has been running on continuous evaluation, for example, do incorporate social media ——

Mr. LYNCH. All right.

Ms. COBERT.—and we are learning from those pilots.

Mr. LYNCH. This is not the general public, so there should be no hedging. These people want top security clearance in many cases. And that is fair enough, but we obviously have the obligation to vet these people if they are getting this top secret clearance. That is all I am saying.

Ms. COBERT. We share that commitment, Congressman, and I'm sure the DNI shares that as well.

Mr. LYNCH. Thank you. I yield back.

Chairman CHAFFETZ. And before the gentleman yields back, maybe what we should do is take all the data and put it on an Apple iPhone because evidently, that is encrypted. That would be a heck of a lot cheaper than trying to recreate what Apple is evidently able to do, so just an idea.

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

Mr. MEADOWS. Thank you, Mr. Chairman. Thank each of you for your testimony. Thank you for your work.

Mr. Halvorsen, let me come to you because, as I understand it, you are the CIO and you report to whom?

Mr. HALVORSEN. I report to the Secretary of Defense.

Mr. MEADOWS. And so as we go to implement this new process, it is your responsibility, the funding—you make the decisions, is that correct?

Mr. HALVORSEN. That is correct.

Mr. MEADOWS. Okay. Then help me understand because OPM has a relationship here, so how, now that it is your decision and we are going to pay for it through OPM, how do the two of those work together because it seems like the funding stream now is going to be, I guess, separated so to speak.

Mr. HALVORSEN. Very clear. The funding stream that we have talked about, the $95 billion is for the build of the new system. It is not the entire funding stream for the operation of the NBIB.

Mr. MEADOWS. So Ms. Cobert has the funding for the operation?

Ms. COBERT. The funding for the operation of the Federal Investigative Service is a—it is a fee-for-service operation. So DOD, when it requests a security clearance ——

Mr. MEADOWS. Right.

Ms. COBERT.—pays the Federal Investigative Service and will pay the NBIB as that bureau is stood up to conduct the investigations. So the funding for the investigations we do for DOD actually comes from DOD. The fundings we do for other Federal agencies come from them. It is a revolving fund model as opposed to an appropriated model.

Mr. MEADOWS. All right. So how does that affect oversight and really as we start to look at it? Because when it gets in to be a fee for service, why would they contract with OPM? Is that a contract they have to have with OPM or can they go to an outside source? I mean, you see where I am going with this, the potential conflict.

Ms. COBERT. Sure. The agreements we have in place, the way we—it is—will be structured with the NBIB is that the NBIB will conduct the background investigations for DOD and other agencies, as we do today. We charge them a price for those ——

Mr. MEADOWS. Sure.
Ms. COBERT.—investigations ——
Mr. MEADOWS. Right.
Ms. COBERT.—and even today, we work closely with DOD as our largest customer and with the other PAC agencies around pricing. We want to make sure we are doing a quality job but we are doing it in a way that is a smart use of taxpayer dollars.
Mr. MEADOWS. Well, and I see that. I guess, Ms. Cobert, one of the concerns I have is when you have monies that are going to OPM versus an outside contractor, whomever it may be, the accountability, it is kind of like having a general contractor that has subcontractors that are—who is ultimately—if the job is not done correctly, who ultimately—who does that fall to? Does it fall to Mr. Halvorsen or to you? And ——
Ms. COBERT. The operations—the investigative operations will be housed in OPM. They will be—report to me. I will be accountable.
Mr. MEADOWS. All right. So how do you anticipate—you know, if it is a fee for service, how do you get the appropriations to make sure you are properly staffed to be able to—you know, because, again, it becomes a model that becomes extremely tricky. It is operating like a private sector, but yet, you are not.
Ms. COBERT. Again, the model that was put in place to have a fee-for-service model is because the agencies, who are the ultimate customers of background investigations, fund those. They are in fact demanding customers. When we work with DOD today, we have an ongoing dialogue about what are we doing with their funds? How are we carrying that through?
We—agencies' demands for background investigations are somewhat unpredictable. They give us expectations but their level of demand for background investigation is a result of their activity, and so they pay for those, and we use those funds ——
Mr. MEADOWS. Okay. But so why would we not just say, okay, Ms. Cobert, you have all the authority? Why do we do this back-and-forth fee aspect of it because it just seems like a shell game where we are moving it from one area to the other, and why wouldn't we just say you are responsible, you are accountable from an oversight, appropriations, and everything else? This back-and-forth becomes very problematic.
Ms. COBERT. We are responsible for the use of the revolving funds in our congressional budget justification.
Mr. MEADOWS. Right.
Ms. COBERT. We talk about the amount of the revolving funds that we anticipate using in fiscal year 2017. We work the pricing through with our interagency partners, so we are responsible for the spending of those funds. The amount that we put to work in the revolving fund is part of our budget submission.
Mr. MEADOWS. But do you see my point that if he comes back and he says, well, I only had demand for X number of—it creates a problem for you instead of—do you follow me?
Ms. COBERT. That is an exact issue ——
Mr. MEADOWS. It is ——
Ms. COBERT.—we have, and that is why we work with agencies to understand what are their projections, what are they doing, what do they need.

Mr. MEADOWS. Okay.

Ms. COBERT. We do want agencies to actually, you know, understand what it takes to do this, and that's—I think this structure works well from that perspective. But part of standing this entity up, we've done some excellent work with the CAPE group at DOD about how to fund this, and we are going to continue to look at that, and I'm happy to continue that dialogue as we go forward.

Mr. MEADOWS. Okay. I am out of time. I want to remind all of you that Mr. Connolly and I are going to be looking very closely at FITARA, and while I have you here, I want to emphasize it once again. I yield back.

Mr. RUSSELL. [Presiding] The chair now recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman. And let me take up where my friend from North Carolina left off. We are going to follow up on FITARA.

Ms. COBERT. Our FITARA plan has been approved by OMB.

Mr. CONNOLLY. And conveniently, Ms. Cobert, we have OMB right here. But I do think there is bipartisan consensus on a lot of the IT aspects of Federal management, and that may not last forever, but we are working hand-in-glove and seamlessly on this committee and our two subcommittees with respect to that. And I pray you take advantage of that because anything can happen, you know.

Mr. Halvorsen, I think you had a personal loss in your family, is that correct?

Mr. HALVORSEN. That is correct, sir.

Mr. CONNOLLY. I am so sorry.

Mr. HALVORSEN. Thank you.

Mr. CONNOLLY. And you were supposed to be at an event with us the other day, and all of us, everybody there wanted to convey their sympathy to you and your family.

Mr. HALVORSEN. I thank you, and I appreciate the scheduling you've made to ——

Mr. CONNOLLY. We understand perfectly of course, and I hope your family is doing okay.

And, Ms. Cobert, congratulations on bringing us together. Hopefully, it will have some effect in the other body. And I commend the chairman and the ranking member. Especially if we are as concerned as we say we are about the breach at OPM, the last thing in the world we need is any cloud at all over the legitimacy or status of the head of OPM, and so I would pray our colleagues in the other body confirm you as swiftly as possible. There is no substantive reason not to do that, and I know you have been working very hard in your acting capacity to try to deal with some very heavy baggage ——

Ms. COBERT. Thank you.

Mr. CONNOLLY.—with respect to breaches. And I will say, I know my friend from Florida was expressing some frustration, but I also am one of the victims. And my experience with the service provided so far has been very positive.

Ms. COBERT. Thank you.

Mr. CONNOLLY. They have caught things we didn't know about. In fact, frankly, they are so strict they are—you know, my wife

can't always respond in my name to their concerns, so they are pretty tight. So hopefully, that is the experience of others as well. And as I have told you privately, we have, I don't know, 20-something million victims through no fault of their own, and priority number one of OPM and you as the Director is to protect those victims and make them as whole as we can. And I know you share that goal as well.

Mr. Halvorsen, I am looking at the Bureau's cyber infrastructure and the new plans, and the Office of the Secretary issued this statement, that the purpose of the new design and build for that infrastructure is to "avert or eliminate the continuous and dynamic threat of identity theft, financial espionage, other attacks on personal information while providing a secure basis for background investigations necessary for the Federal Government."

Can you briefly describe the mission of the Defense Information Systems Agency and why it was selected to design and operate that new system to meet that goal?

Mr. HALVORSEN. This is the DOD's contract acquisition and design agency for major systems in an IT. In my review of the capabilities, DISA was best positioned to be the oversight and designer of this.

I will stress, however, when we say DISA is the designer of this system, it will not be without lots of input, and in some cases, commercial adaptation of technology.

Mr. CONNOLLY. Will this new network or system deploy EINSTEIN sensors for protection?

Mr. HALVORSEN. It will deploy the right set of sensors. It could be EINSTEIN. It could be EINSTEIN equivalence or things that might be better than EINSTEIN as we're looking at the future. As you well know, this is a field that changes rapidly. There will not be a single system that does this, but an integrated layer of systems that are better integrated to talk and both stop attacks, but if they had happened, to identify them and quarantine them quickly.

Mr. CONNOLLY. All right.

Mr. HALVORSEN. That takes a layered defense system.

Mr. CONNOLLY. I am going to run out of time, and if the chairman will allow them to respond, I will of course give up my time.

But, Ms. Cobert and Mr. Halvorsen, when the breach occurred, one of the things we were told was, well, OPM had deployed EINSTEIN 1 and EINSTEIN 2 but not EINSTEIN 3. And had it had EINSTEIN 3 in place, maybe the breach would have been mitigated or eliminated. I would like both of you to comment on that because I think there is a lot of confusion up here, which I share, well, is EINSTEIN the answer or is there some other answer? Are there things that DOD that are not yet available in the civilian agencies that should be? Help us a little bit with that—do we still stand by that analysis?

Ms. COBERT. Congressman, what I can tell you is we continue to be moving forward with deploying the EINSTEIN capabilities as they become available. So we have been moving forward with EINSTEIN 3 and EINSTEIN 3A. From my perspective at OPM as a customer of the support that folks like DOD and DHS can provide, I am happy to be an early adopter of the smart tools as they make

them available to us. And whichever are the best tools, and folks like Mr. Halvorsen will help us figure out what those are, those are the ones we will deploy.

Mr. HALVORSEN. I think Beth got it right, sir, and I think you know we will continually review this. We've had recent reviews by—frankly done on behalf of what I've asked. NSA and some commercial customers say these are the best-layered defenses today. EINSTEIN technology will be part of that, but it is not the singular answer to build the best defense system forward.

Mr. RUSSELL. The gentleman yields back.

The chair now recognizes the gentleman from Georgia, Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman.

Mr. Scott, just out of curiosity, will the President's appointee to the NBIB be confirmed by the Senate?

Mr. SCOTT. As proposed, I don't believe so, sir.

Mr. HICE. Do you know how that process will be? Is it just an appointment ——

Mr. SCOTT. That's correct.

Mr. HICE. Okay. Ms. Cobert, let me go back to you. As you know, the PAC conducted the review after the Navy yard shooting. That review led to 13 specific recommendations to improve the clearance process. Has the intelligence community fully complied and addressed those recommendations?

Ms. COBERT. Congressman, the PAC collectively has been working to implement the full set of recommendations from the review following the Navy yard.

In my prior role at OMB when I was the chair of the PAC, in my current role as acting Director of OPM, we've been working closely with our colleagues in the DNI, for example, to put in place pilots of continuous evaluation to implement new Federal Investigative Standards, to improve access frankly ——

Mr. HICE. So are you saying ——

Ms. COBERT.—so we are working ——

Mr. HICE.—they have or have not been ——

Ms. COBERT. We are ——

Mr. HICE.—fully implemented?

Ms. COBERT. We are working through the process. The timetable for full implementation is not—we're still in that process but we are actively working that and actively managing it through the PAC.

Mr. HICE. So it has not yet been fully implemented, and you do not have a time frame ——

Ms. COBERT. There are ——

Mr. HICE.—we know it will be complete?

Ms. COBERT. There are different time frames for different elements. So one of the elements was to actually have continuous evaluation pilots in place. We have those in place. DOD has done some that's covered hundreds of thousands of people. The investigative standards and the quality ——

Mr. HICE. All right. Can you give us ——

Ms. COBERT.—of the standards ——

Mr. HICE.—a general time frame?

Ms. COBERT. Some of the elements are already due. Some last until 2017. I can—I am happy to provide you. We report on Performance.gov ——

Mr. HICE. Please provide that and let's carry on, but please provide that information.

Ms. COBERT. And we would be happy to do that, sir.

Mr. HICE. All right. The Navy yard shooter had multiple previous arrests and yet was still somehow able to obtain clearance. How can this be?

Ms. COBERT. Congressman, there are real challenges in getting complete and comprehensive records from local law enforcement. Some of those are due to the challenges that the local law enforcement has in their own recordkeeping.

Mr. HICE. Okay. There has been recommendations ——

Ms. COBERT. Those systems aren't automated.

Mr. HICE.—to work and improve that process from State and local criminal records. When is that process going to improve?

Ms. COBERT. That process has seen improvement. I can cite examples from New York City, from—we track actually ——

Mr. HICE. I don't want examples. I want when are we going to see that enormous gap closed?

Ms. COBERT. We are continuing to work with law enforcement. The records are their records. Things like Congress gave us with the NDAA that gives background investigators greater access to records that was implemented last year will be one step in helping us, but we have to work this through with local law enforcement to make sure they've got ——

Mr. HICE. That is the whole point.

Ms. COBERT.—the systems.

Mr. HICE. That is the whole point. The local law enforcement, when is that relationship going to be resolved so that information can be readily made available so that we don't have people like the Navy yard shooter gain access?

Ms. COBERT. Congressman, we are working actively with local law enforcement. In fact, we have—we had ——

Mr. HICE. Okay. Listen, that ——

Ms. COBERT.—a task force, and we are going to ——

Mr. HICE. That is ——

Ms. COBERT.—continue that.

Mr. HICE. That is a really cheap answer. We are working actively. We are working actively, and yet—please provide that for us. I want as much specifics as you can provide without rambling ——

Ms. COBERT. I'm happy to provide you that.

Mr. HICE.—on this issue.

Mr. HICE. All right. Have the revised 2012 Federal Investigative Standards been fully implemented?

Ms. COBERT. We have implemented those through Tier 3. The rest of them are on schedule to be implemented over the next year too, I believe—I don't have the specific timeline but had ——

Mr. HICE. Okay.

Ms. COBERT.—implemented the Tier 3, for example, this fall.

Mr. HICE. Okay. Another recommendation involved the detection of false information that was submitted by applicants. As you may

recall, Snowden, for example, said that he had worked for the U.S. Government for 6 years, investigators and all that, never contacted any coworkers, they never got any further details. The Navy yard shooter has serious mental health problems. What is being done to verify applicants' information more complete and in a more effective manner?

Ms. COBERT. So there is a number of steps that we've put in place to increase the accuracy. I can go through the specifics and probably get that back to you in terms of each of those elements because that involves work with the different—I don't have the details of that right here ——

Mr. HICE. All right. So you ——

Ms. COBERT.—but I can get that to you.

Mr. HICE. Doesn't it seem that that would be information that you would have?

Ms. COBERT. I want to make sure that my response to you in—is accurate in terms of exactly the specifics of the progress we've made, sir.

Mr. HICE. Okay. And we are talking about applicants putting false information and no one checking it. That seems like that would be information, if it is being corrected, that would be right on the top of your head. I would appreciate you getting that information to us ASAP.

My time is expired, Mr. Chairman. Thank you, and I yield back.

Mr. RUSSELL. The gentleman yields back.

The chair now recognizes the Congressman from California, and I appreciate his efforts on this issue, Mr. Lieu.

Mr. LIEU. Thank you, Mr. Chairman.

The hearings last year in Oversight Committee exposed fundamental weaknesses in our nation's IT infrastructure, specifically as applied to OPM. And thank you, Mr. Scott, for doing the 100-day cybersecurity sprint last year. The Director of the OPM last year resigned to be replaced by Ms. Cobert, and you have been doing a terrific job given the situation you have been put in.

And last October, Representative Russell and I wrote a letter to the administration to the PAC board saying you need to move the security clearance IT system to the Department of Defense. And I am very pleased to read in your testimony, Ms. Cobert, that in fact the Department of Defense, with its unique national security perspective, will design, build, secure, and operate the security clearance IT system.

My question has to do more with the other aspect of your plan, which is now the creation of a new bureau, the National Background Investigations Bureau. And I share some of the concerns raised by Congressman Russell. And my first question has to do with the wiring diagram. My understanding is this bureau will be headed by a Presidential appointee who then reports to the Director of OPM. Still, Ms. Cobert, could you or the new Director fire that person?

Ms. COBERT. I imagine I could, yes, sir.

Mr. LIEU. Okay. What happens if you have a disagreement with the Department of Defense over how to do the security clearance IT system?

Ms. COBERT. Congressman, as Mr. Halvorsen said, DOD has the responsibility for the security of the IT systems. We have given that responsibility in agreement with them because we want to rely on their expertise. They have the national security expertise, the cybersecurity expertise around these issues. They are in that place because of that expertise, and we would expect that their guidance on how those things should operate is what we would follow.

Mr. LIEU. And if they want more money to do the IT system upgrades and so on, where would that money come from?

Ms. COBERT. So let me distinguish between the budget funding for the IT upgrades, as Mr. Halvorsen has described, as well as the funding for the ongoing support for NBIB. The funding for NBIB, because it is a fee-for-service model, are fees paid for our customers. The largest customer of the National Background Investigations Bureau will be the Department of Defense. And so, in fact, DOD will be providing those funds to the NBIB through the payments that they make for background investigation services. So they are both the customer paying the bill, as well as the individuals who will be supporting the use of those funds on IT for the revolving nature of the funds.

Mr. LIEU. Okay. In terms of personnel, my understanding is the Federal Information Service will be folded or basically replaced with this new bureau. Will there be less people, the same, or more?

Ms. COBERT. Congressman, I don't have the answer to that question at the moment. We are working with NBIB to make it purpose-built for this mission, for the scale of this mission, for the new capabilities, and frankly, for the new operating practices that are going to be part of it.

In addition to the IT redesign that DOD will be leading, a key part of the transition team and the ongoing efforts is business process reengineering. How do we take advantage of these new technology tools to make this process be better, be smarter, be more efficient? And so when we put together, we can't tell you today what the scale of the individuals involved will be.

Mr. LIEU. And taking a step back, what is the reason for not continuing with the Federal Investigative Services? Why do we need this new bureau?

Ms. COBERT. Beyond the changes in how we operate IT, which are significant and particular given the IT intensity of this activity, that is a very significant change. What we wanted to do with the other change is to elevate the mission, elevate this role by having a Presidential appointee lead it in conjunction with the PAC as a peer of those leaders.

We want to make sure that it has more dedicated support custom-tailored to this mission to make sure we can address the privacy issues with a national security context to make sure that it's got greater dedicated resources for the specific and unique type of contracting activity that it does or the legal issues it confronts or the other key elements of its operation.

So we wanted that dedicated support, and we wanted to make sure we could institutionalize the interagency collaboration that really works. We work closely through the PAC with the IC, with the Department of Justice with the FBI, and that will be embedded in how the NBIB operates.

Mr. LIEU. Thank you. And I yield back.

Mr. RUSSELL. The gentleman yields back.

The chair now recognizes the gentleman from Alabama, Mr. Palmer.

Mr. PALMER. Thank you, Mr. Chairman.

Mr. Evanina, what sort of records do current continuous evaluation pilot programs look at?

Mr. EVANINA. Well, sir, I could speak for the intelligence community and the Office of the Director of National Intelligence. We're looking at about seven or eight major databases that will be continuously evaluated to identify areas of concern for clearance-holders that currently exist and on a continuous basis.

So, for instance, right now, background investigations that are reinvestigations occur either a 5-year or 10-year cycle. We're looking to facilitate that on a continuous basis so, for instance, if you have an incident tonight, a domestic dispute, an arrest or financial issue like bankruptcy, we'll identify that immediately and not have to wait for 5 years to do that. But there'll be automated checks on a recurring basis.

Mr. PALMER. Would you be able to follow up on something like with Mr. Alexis where he showed that he lived in Seattle but worked in Manhattan? Would it pick up discrepancies like that?

Mr. EVANINA. Probably not specifically where he resides, but the request for public information of residency would be part of that documentation. However, what happened with the law enforcement issue on the West Coast would not be a part of that. There'd be financial records, travel records, and publicly available records on the internet.

Mr. PALMER. The personnel that are looking at these documents, does it not make sense to train them to look for abnormities like that? I mean, to say that you live in Seattle and you work in Manhattan should at least ask someone if they are commuting.

Mr. EVANINA. Absolutely, sir. And I'll—I'm confident that it happens now when investigations are conducted on background investigations and reinvestigations periodically with their 5- and their 10-year period. Those investigators who conduct those investigations are robust and thorough and they would ask that question, sir.

Mr. PALMER. Mr. Halvorsen, what records does the DOD pilot program look at?

Mr. HALVORSEN. Sir, all of the same records plus we are looking at financial, we're working with law enforcement to do some criminal and sex offender. We look at social media, other internet public records and internal DOD data sources.

Mr. PALMER. I want to go back to Mr. Evanina. Given that it has been almost a decade, why is the continuous evaluation not yet a standard practice across the intelligence agencies?

Mr. EVANINA. Sir, I'll proffer that a lot of agencies in the intelligence community currently utilize continuous evaluation.

Mr. PALMER. You said a lot of them, but why is it not standard practice across all of them?

Mr. EVANINA. I'll correct that. The majority if not all of the organizations in the intelligence community currently use continuous

evaluation. We are working with partners here to promulgate that across the executive brach of the government.

Mr. PALMER. I appreciate that it is a majority, but can we get to all?

Mr. EVANINA. Yes, sir. I'll get you specifics as to which agencies don't if there is such an agency that does not conduct that now.

Mr. PALMER. Thank you, sir.

Mr. PALMER. I want to go back to Mr. Halvorsen. Is the information looked at under the pilot program different from what would be looked at under the periodic reinvestigations of the current standard practice?

Mr. HALVORSEN. The data is different, and that's part of what we're trying to pilot. There are some additional data sources in the pilots, and that's what we're evaluating now to see if that makes more sense in a continual way in cooperation with our intelligence counterparts.

Mr. PALMER. When will all of the DOD's cleared population be covered by the continuous evaluation program?

Mr. HALVORSEN. Sir, I think there are two questions there. Right now, the DOD, we do use continuous monitoring. We are still in the process of working with the intelligence community on when that will become the standard for periodic investigations.

Mr. PALMER. I want to shift gears a little bit here. Ms. Cobert, at your Senate nomination hearing, you said that the changing nature of cybersecurity means we all need to change the way we interact, the way we use systems at work and at home. You then explained that you yourself cannot access your personal Gmail account from your OPM computer because that is the way a lot of threats come in. Can you expand on how access to private accounts like personal Web mail on agency computers compromises the integrity of the Federal information systems?

Ms. COBERT. Certainly. The—by—there's—whether it's phishing attempts or other things, there's a lot of ways things come in. Those might not have the same screens and filters that we have on our own government emails. And so the policy that we've put in place at OPM is to restrict access to those personal accounts. You don't want individuals being able to click on those accounts and accidentally click on something as a phishing attempt, for example.

We know about the security controls on our own systems. We don't know about the security controls on individual's personal emails. Therefore, we do not want them on OPM computers.

Mr. PALMER. Okay. My time is expired, Mr. Chairman. I yield back.

Mr. RUSSELL. The gentleman yields back.

The chair now recognizes the gentleman from California, Mr. DeSaulnier.

Mr. DESAULNIER. Thank you, Mr. Chairman. I want to thank all the panelists for the hard engaged work you are in the process of. Certainly, I think we can all agree that this was a very important issue, and the OPM data breach was alarming to say the least. So my questions and comments are going to be more directed to that understanding where responsibility lies, sort of consistent with some of the comments by Mr. Meadows.

Understanding that this wasn't an isolated incident and it was sophisticated and coordinated and those kind of things are going to continue to happen in our new world. And so I have a couple of slides if we can put the first one up, speaking of technology.

[Slide.]

Mr. DESAULNIER. Our committee investigations found that cyber attackers used a sophisticated kind of malware called PlugX.

Slide 2, please.

[Slide.]

Mr. DESAULNIER. The cyber attackers targeted government contractors with access to large amounts of personal information about Federal employees. These contractors, as you can see in the slide, were KeyPoint, which connected to OPM for the background investigation work it does, Anthem and Premera, which provide insurance to millions of Federal employees and their families.

Slide 3, please.

[Slide.]

Mr. DESAULNIER. Once they hacked into KeyPoint, as we have now learned, the attackers were able to disguise their movements to appear to be authorized users inside OPM's networks. Once they got in, they installed PlugX malware on OPM's networks as well.

Slide 4, please. This is the last slide.

[Slide.]

Mr. DESAULNIER. Over a period of months in 2015 the attackers made off with personal information they found using this method. In all, again alarming, over 90 million people could have been affected by this breach.

Mr. Scott, at the committee's first hearing—that is the last slide, thank you—on the OPM data breach on June 16 of last year, your written testimony stated, "Both State and non-State actors who were well-financed, highly motivated are persistently attempting to breach both government and nongovernment systems. And these attempts are not going away. They will continue to accelerate on two dimensions. First, the attacks will continue to become more sophisticated"—as we have seen—"and secondly, as we remediate and strengthen our own practices, our detection capabilities will improve so it is a constant effort."

On a scale of 1 to 10, how would you rate, given your experience, the sophistication of the cyber attackers responsible for the breaches of KeyPoint, Anthem, and OPM in 2015?

Mr. SCOTT. I think there's consensus among all of us who looked at it this that it's in the upper ranges, I'd say 8 or 9, in that range.

Mr. DESAULNIER. Thank you. Director Cobert, our understanding is that cyber attacks against OPM were underway in 2013 and 2014, and they were only detected in 2015 when new tools deployed by former CIO Donna Seymour came online, is that correct?

Ms. COBERT. That is my understanding, yes, sir.

Mr. DESAULNIER. In your opinion, could OPM have prevented these attacks with the tools it had in 2013?

Ms. COBERT. The tools we had in 2013 are very different—were not adequate to prevent the breach. The breach occurred, correct?

Mr. DESAULNIER. Right.

Ms. COBERT. Yes.

Mr. DESAULNIER. So in the overall context, this is the constantly trying, stay ahead of things, and that OPM was trying to stay ahead, but the tools they had weren't sophisticated enough to stop it so we slid behind.

Mr. Halvorsen, the committee's investigation revealed that the adversary behind these attacks, again, were sophisticated and persistent and will continue to be. As these breaches illustrate, the adversary can be and will be present and at work, laying low, and being invisible largely to us. Knowing that we all have a lot of confidence in DOD and knowing it is not misplaced, I think, in bipartisan level and knowing that you can't explain everything in the sophistication that you bring to this endeavor, the molding between you and OPM is important.

So could you just briefly describe with obviously being sensitive to the classified issues that you deal, what do you bring in a nutshell to this effort that will give us a higher level of confidence.

Mr. HALVORSEN. Well, I think, first of all, DOD, we live with a volume of attacks and I won't give the specific numbers. You—I think you've seen them. They're very, very large every day from everything ranging from the less talented to the most extreme talented adversaries. Our integration across DOD and how we deal with that both in preventing them but also—and I want to stress—people keep attacking—I don't think we're at all going to have a perfect system of prevention. Our ability to quickly detect, isolate, quarantine, and take corrective action and protect the forensics is something we will bring to this table and probably the integration of all of that and being able to produce a better full environment is what DOD brings to the table.

Mr. DESAULNIER. I just want to thank you all. You are a group of Federal employees that when you are doing your job well, nobody hears from you, so congratulations. Thank you, Mr. Chairman.

Mr. RUSSELL. The gentleman yields back.

We do appreciate the panel and their efforts. I would like to just make some closing comments. The fee-for-service, while it is understood that you have users and the compensation should come from those that use, but could you please explain, whoever would like to address it, where you have $95 million now that will come from Department of Defense, and yet Department of Defense will still be required to do a fee for service for their own users? So not only do they get to pay, they get to pay again. They have complete responsibility but they don't have the authority. Is that accurate?

Ms. COBERT. Congressman, the $95 million requested in the budget was to deal with the modernization and move to a new model. That is a—someone will think of that as the—more the one-time investment that we need to make on behalf of the entire Federal Government, and because DOD will be doing that work on behalf of the government, the funds were put into the DOD budget.

On an ongoing basis, it is our responsibility working with DOD to make the overall operations and systems work well. DOD, as Terry has stated, will be the lead, will have authority for the decisions around the systems. We will then at OPM, through the NBIB and with our interagency partners, be deploying those systems every day to conduct the work. So DOD will be building and oper-

ating the system, securing the systems. At NBIB we will be using those systems to conduct the investigations, and the fees from agencies support that work so that we have the funding to get it done.

Mr. RUSSELL. Well ——

Ms. COBERT. It means you can scale that as the demand changes.

Mr. RUSSELL. And I understand that, and I appreciate that, Director Cobert, but, I mean, doesn't it stand to reason that if you are the one providing the service, you ought not to charge yourself to perform it? Would you agree with that statement? The Department of Defense will be conducting what amounts to its own background usage, and yet now, you are also requiring a fee for them to perform their own service. Is that correct?

Ms. COBERT. The Department of Defense will be provisioning the IT system. The individual investigators, the work that's done in using those systems will be done by the NBIB. So they're our IT provider. We are the users, and that's what the fees cover.

Mr. RUSSELL. Okay. But herein is the concern. You know, while you have, you know, a great reputation and, you know, as you have heard in the comments in committee today, you know, good bipartisan, you know, commendation for your efforts, all of that could change in a year.

The whole team that we see, although they are longstanding public servants and we appreciate that service, if we don't set this structure up correctly and, as we heard by admission from Mr. Scott today, this funding is going to come from the top line of Defense. Well, gee, you know, as I have already illustrated, that amounts to about 60,000 soldiers' pay.

This is a problem because we are trying to set up a system that will have competing interests that will go against something that comes top line from defense, and then it appears that the Department of Defense, which will have much of the legwork and will provide much of the sweat equity so to speak, they will also be asked to pay for their own labor.

Ms. COBERT. Congressman, I—I'm not sure I agree with the competing interest point. DOD is our largest customer. We are providing services to DOD. They as our customer—and I can attest today they are a very demanding customer, want to make sure that we do a quality job, that NBIB will do a quality job and that NBIB does that in a quality way but in an efficient way. We have dialogues with them today about pricing. This activity does have to happen across the Federal Government. It is an important activity. It has a cost, and we believe that this structure of us working with DOD and our other customers puts appropriate pressure on NBIB to do it right, to do it efficiently, and that will continue. I actually view that more as an alignment of interests ——

Mr. RUSSELL. Well ——

Ms. COBERT.—than a competition.

Mr. RUSSELL.—and I get that from a government function point of view, but I think the real issue here is that this is a national security issue. It has been breached. It will last, in my estimation, at least two generations. There is a gold mine of information whereby to track folks.

And so the big concern of mine is is that, you know, from a—and I don't mean this in an unkind form but in a technical form—from a bureaucratic view that, yes, there are government functions, but since this is such a national security issue, it stands to reason that many of the three-letter agencies did not want to be slid under OPM when we did these reforms originally. In fact, they stiff-armed it. They didn't get breached.

Department of Defense, largely through pressure of Congress and through budgets, did. Now, we are turning back to them but we are still going to keep it potentially in a convoluted authority structure. This is a defense issue. This is a national security issue. And it still begs the question of whether or not DOD should be involved in its own personnel at all under an OPM structure. And I think those questions have to continue to be asked. I am very concerned about that.

And I would just be curious both from Mr. Evanina and also Chief Halvorsen in that regard would we have better security for our defense personnel in a standalone or do we need to have this amalgam of agencies with a convoluted structure, cooperation notwithstanding, that could make us vulnerable yet again in the future. Chief Halvorsen?

Mr. HALVORSEN. So I think what we've proposed is actually the best security solution. We are, from DOD's standpoint, in a sense acting as the contractor for their IT services. We will provide those. We are responsible for those IT services.

And I want to make a couple points. The cost for the current IT are baked into the current OPM pricing. The $95 million is to do the modernization. I actually believe when we are done with the modernization, the IT cost will actually come down. This is a more effective way to do IT than what we have been doing today. The IT will be central. Everybody will use standard—the IT system.

I think the same thing is true as we look at the business systems. I don't think you want DOD, Department of State, anybody else, doing different things with the investigations. I think that A) makes it more efficient, but also creates seams that could be exploited. I think we eliminate those seams.

I understand your issues about are we going to be able to get the right authorities in place. I think we are, and I think we will owe you continual updates on how we're doing it.

Mr. RUSSELL. Mr. Evanina?

Mr. EVANINA. Sir, I will echo that and say that from the intelligence perspective from the community, we believe this is the most effective and efficient manner to attack this problem. And I think it's important to bifurcate the issues here. The first half of it is the investigations being done in the field to include Federal employees and contractors and the adjudications, which is inherently governmental by the folks at the NBIB.

The second part of that is the systems and data that's acquired to be securely stored by DOD we believe is the most efficient way to handle this issue not only from a national security perspective and housing the data and ensuring it's secure through DOD but also maintain the current rhythm and motive of doing the investigations we are currently doing now.

Mr. RUSSELL. I would like to thank panel. We appreciate both your time and your continued efforts in this. It is appreciated. We all care about the same things. It is my sincere hope that we will work together to resolve these issues that have come up.

And seeing that there is no further business, this hearing is now adjourned.

[Whereupon, at 12:01 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Opening Statement
Committee on Oversight and Government Reform
"Security Clearance Reform: The Performance Accountability Council's Path Forward"

Thursday, February 25, 2015

At last count, the Director of National Intelligence reported **4.5 million people** held security clearances.

And the queue for a clearance continues to grow.

At the end of fiscal year 2015, there were more than 388,000 new background investigations and 117,000 periodic reinvestigations backlogged at OPM.

That is a lot of folks with access, or requesting access, to our most sensitive national security information.

And we learned last year that most – if not all – of the personal information collected during background investigations was exfiltrated in one of country's biggest cyber attacks.

We cannot let this happen again.

We have to fix the process and we have to protect the information we collect.

The process we use to determine if someone is eligible for a security clearance is broken.

A number of high-profile events have illustrated just how broken the process is.

- Edward Snowden openly discussed his hatred of federal surveillance for years while holding a Top Secret clearance.

- The Navy Yard shooter Aaron Alexis was granted a Secret clearance despite multiple arrests and a troubled psychological history.

The failure to detect these obvious problems cost us some of our most sensitive national secrets and a number of lives.

As the process for evaluating security clearance applications has evolved, we've experimented in a number of ways in attempts to improve it.

The Defense Investigative Service at the Department of Defense was created in 1972 to house the process for issuing security clearance credentials.

Under President Bush, in 2004, almost everything – both process and data – was transferred to OPM.

When that transfer occurred, OPM started contracting out the investigative work.

In the last few years, one contractor in particular received a lot of attention for its shoddy work: the United States Investigative Services or "USIS."

In fact, USIS was the same contractor that approved the security clearances for both Edward Snowden and the Navy Yard shooter.

In 2013, the OPM OIG reported USIS fraudulently submitted security clearance investigations to OPM without conducting a thorough quality review as its contract required.

One egregious example included a USIS employee who "completed 15,152 case reviews during a one month timeframe, with most of these occurring within minutes of each other on multiple days."[1]

The creation of USIS, itself, was an experiment under President Clinton that "spun off" a number of OPM employees to create a private entity owned by those very employees.

The IG reported senior officials at USIS did this "in order to maximize profits" and concealed these fraudulent activities from OPM.

This history teaches us a valuable lesson: ***we shouldn't experiment with how we process and award security clearances***.

[1] US Office of Personnel Management, Office of the Inspector General Office of Audits, Final Audit Report No. 4A-IS-00-13-062.

If we are going to change the way we process security clearances, ***again***, we have to make sure we are improving the process and not creating another problem.

Improving the process means modernizing to account for both new technologies and evolving global threats.

One way to do this is to move to a process of continuous evaluation of security clearance holders, as opposed to re-evaluations every five years.

- Under continuous evaluation, events like criminal arrests or major financial changes would automatically alert an agency that an employee with access to classified information needs updated review.

- Both Presidents Obama and George W. Bush ordered continuous evaluation for individuals with clearances.

- But, the government is still only operating pilot continuous evaluation programs.

Also a problem is the SF-86 form applicants fill out to apply for a clearance

It hasn't been updated since 2010 and is antiquated and nonsensical given our current threat environment.

- Do we really need every address a person has ever lived along with the names of countless people at each location to talk with?

- Yet, we don't monitor an applicant's social media or ask for information about any online identities.

- We ask applicants about their potential sympathies with Communism, but we don't inquire if they feel morally compelled to disclose national security secrets, as Edward Snowden openly claimed on the Internet.

- We need to ask ourselves: are we asking the right questions?

Nothing in the plan put forth to date addresses whether we are going about this in

the right way.

That is an important piece of this puzzle.

Not only do we have a process problem, we have a data protection problem.

The multiple breaches of OPM's system and exfiltration of over 21 million background investigation files highlight the complete lack of adequate cyber security at OPM for this incredibly sensitive information.

It makes no sense as to why 21 million background investigation files were active on OPM's system and available to any hacker.

Files that are not currently under investigation should not be active on the system.

You can't hack what isn't there.

Under the proposed plan, responsibility for the IT infrastructure housing background investigations will be transferred back to DOD.

It is unclear why this can't occur at OPM.

Protecting this type of information should be a core competency of OPM, which is the government's human resources agency.

In fact, the creation of the "National Background Investigations Bureau" to manage the process and transferring the information it collects to DOD seems more like a marketing tool designed to solve a perception problem.

We need more meat on the bones of the current proposal.

We also have a problem with the current Acting OPM Director's appointment.

The OPM IG recently notified Ms. Cobert her appointment was in violation of the Federal Vacancy's Act, opening any decision she makes to a court challenge.

Personally, I am hopeful Ms. Cobert can provide desperately needed leadership to a very troubled, yet important, government agency.

But it's impossible to lead when every decision she makes is open to being challenged.

I appreciate the witnesses being here today.

I look forward to hearing how they propose we make real progress in improving the issuance of security clearances and ensuring the information collected remains safe and secure.

Vitter: Time for OPM to Fess Up on Washington's Obamacare Exemption

Vitter announced he's blocking Cobert's nomination until answers received

(Washington, D.C.) – Today, U.S. Sen. David Vitter (R-La.) announced he is blocking Beth Cobert to be Director of the Office of Personnel Management (OPM). Additionally, Vitter sent Cobert a follow up letter in light of her failure to respond to his February 3, 2016 letter, which requested information regarding Washington's Obamacare Exemption. Vitter said he'll continue blocking Cobert's nomination until she responds to his request for information.

"As much as federal bureaucrats enjoy hiding behind layers of red tape, we have now reached the point where OPM can no longer avoid explaining how Congress was allowed to purchase health insurance as a small business – when it clearly is not," said Vitter. "Ms. Cobert's nomination will not move forward in any capacity until the American people have received answers as to why Washington's Obamacare Exemption exists."

As Chairman of the Senate Small Business & Entrepreneurship Committee, Vitter has been investigating how the U.S. Senate and U.S. House of Representatives were allowed to apply to the DC Healthlink small business exchange in order to receive special Obamacare subsidies available for only small businesses. Click here to read more.

On February 10, Vitter sent a letter to John Koskinen, Commissioner of the Internal Revenue Service (IRS), requesting clarification as to whether Congress is a large employer or a small employer in regards to Members of Congress and congressional staff receiving health insurance under the Affordable Care Act. Congressional employees have started receiving new IRS tax forms that contradict prior claims that Congress is a small business, with Congressional employees also receiving a special taxpayer-funded subsidy that is unavailable to other Americans at the same income level. Click here to read more.

In addition to his previous questions, in his letter, Vitter asks Cobert to confirm whether Congress is a small business or a large employer. Click here to read Vitter's letter.

-30-

U. S. SENATOR
David Vitter

CHARRTS No.: HOGRC-01-001
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Russell
Witness: Mr. Halvorsen
Question: #1

National Background Investigative Bureau

Question: Is NBIB envisioned as a consolidation of existing capabilities under one authority or is this an opportunity to build a purpose-driven system from the ground up?

Answer: The creation of the NBIB is an opportunity to build a purpose-driven system from the ground up. The NBIB transition team will conduct business process reengineering activities to define the background investigation process and the requirements the Department of Defense will use to build the new system

CHARRTS No.: HOGRC-01-002
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Russell
Witness: Mr. Halvorsen
Question: #2

National Background Investigative Bureau

Question: What best practices are you leveraging from relevant industry thought and technology leaders?

Answer: The Department of Defense is still early in its review of the current OPM systems and planning for the new system development. The Department of Defense intends to use model-based agile system development that will combine industry and government best practices and best of breed commercial products for cybersecurity. In addition to leveraging the Department of Defense's system development and cyber expertise, we will engage with industry and technology leaders through our expected development and support contractors.

CHARRTS No.: HOGRC-01-003
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Russell
Witness: Mr. Halvorsen
Question: #3

National Background Investigative Bureau

Question: What successes and challenges are you facing with implementing a Continuous Evaluation of Cleared Personnel program?

Answer: Successes: The DoD committed to process 100,000 individuals in calendar year (CY) 2014, 225,000 in CY2015, 500,000 in CY2016, and 1,000,000 CY2017. The program has met the goals for both CY2014 and CY2015 and is on schedule to meet the goal for CY2016.

Challenges: To date, funding for the DoD Continuous Evaluation (CE) program has been year-to-year. DoD will continue to seek sustained program funding across the Future Years Defense Program to mature the CE Program, which will enable DoD to leverage the automated records checks capability being developed to support CE to also replace elements of the Tier 3 (SECRET) investigations.

CHARRTS No.: HOGRC-01-004
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Russell
Witness: Mr. Halvorsen
Question: #4

National Background Investigative Bureau

Question: Are you facing any policy or legislative roadblocks in implementing a Continuous Evaluation of Cleared Personnel program?

Answer: The Office of the Director for National Intelligence (ODNI) is developing Security Executive Agent policy guidance that will delineate minimum standards for Continuous Evaluation (CE). This document will enable the Department to more effectively and consistently execute its CE program. In terms of CE program development, DoD and the ODNI are in close collaboration to ensure consistency of effort and prevent duplication. ODNI and DoD are working jointly with various government data providers in an attempt to obtain valuable government information at a reasonable cost at scale. These discussions have been met with varying degrees of success, and may present an opportunity for legislative assistance.

CHARRTS No.: HOGRC-01-005
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Cummings
Witness: Mr. Halvorsen
Question: #5

Contractor Requirements to Report Cyber Breaches

Question: Please identify and provide copies of the contractual clauses DoD requires for each of its contractors detailing the responsibilities of those contractors to report cyber breaches to the Department. In identifying the requested clauses for the Committee, the information that should be provided should include the following: a. The name of the contractor to whom the contract relates; b. To whom the reports must be made; c. What information must be reported; d. How long after a breach is discovered must the report be made; e. Any immunity from liability provided to the contractor for reporting the breach; f. The consequences of non-compliance with any reporting requirements.

Answer: a. The DoD requirements for reporting cyber breaches to the Department are set forth in the DFARS and thus apply to a broad range of contractors and contracts. The Department amended the Defense Federal Acquisition Regulation Supplement (DFARS) on November 18, 2013 to add a new subpart and associated contract clause addressing requirements for safeguarding unclassified controlled technical information. DFARS Clause 252.204–7012, "Safeguarding of Unclassified Controlled Technical Information," required contractors and subcontractors to provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure, and directed contractors to report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems.

On August 26, 2015, DoD issued an interim rule (with a modification published on December 30, 2015) amending the DFARS to implement section 941 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2013 (Pub. L. 112–239) (now at 10 U.S.C. 393) and section 1632 of the NDAA for FY2015 (now at 10 U.S.C. 391), both of which require defense contractors to report network penetrations. Additionally, the interim rule implemented DoD policy on the purchase of cloud computing services. DFARS Clause 252.204–7012 was renamed ''Safeguarding Covered Defense Information and Cyber Incident Reporting,'' and the scope of the clause was expanded to cover the safeguarding of covered defense information and require contractors to report cyber incidents involving this new class of information as well as any cyber incident that may affect the ability to provide operationally critical support. There is a requirement to flow down the clause to all subcontractors who will provide operationally critical support or have covered defense information associated with the performance of the contract. A new clause at 252.239–7010, "Cloud Computing Services," was also added to provide standard contract language for the acquisition of cloud computing services; including access, security and reporting requirements.

b. The DoD Cyber Crime Center (DC3) serves as the single DoD focal point for receiving all cyber

incident reporting affecting unclassified networks of DoD contractors from industry and other government agencies.

c. In accordance with DFARS Clause 252.204-7012, DoD contractors shall report as much of the following information as can be obtained within 72 hours of discovery of a cyber incident:
1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contact or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information

d. DoD contractors shall report to DoD at http://dibnet.dod.mil within 72 hours of discovery of any reportable cyber incident.

e. FY16 NDAA Sec. 1641 provides liability protections to cleared defense contractors reporting cyber incidents under 10 U.S.C. 393, and operational critical contractors under 10 U.S.C. 391. These protections will be further implemented in future revisions to the applicable regulations.

f. Because this is a contract requirement, the normal contract remedies would apply.

CHARRTS No.: HOGRC-01-006
House Government Reform Committee
Hearing Date: February 25, 2016
Subject: Security Clearance Reform: The Performance Accountability Council's Path Forward
Congressman: Congressman Cummings
Witness: Mr. Halvorsen
Question: #6

Contractor Requirements to Report Cyber Breaches

Question: Please identify and provide copies of contractual clauses in DoD contracts that are currently in effect, or that are in the process of being proposed, that would require contractors to cooperate with US-CERT and any other federal agency involved in remediation, in the event of a cyber breach.

Answer: The following clauses require safeguarding of information and reporting to DoD, and under certain circumstances, to other Federal agencies to include the FBI.

DFARS clause 252.204-7012 is used in all new contracts. The clause was effective in November 2013, then updated in August 2015 and December 2015. The clause requires defense contractors to safeguard unclassified covered defense information, to report cyber incidents to DoD, and to provide access to media, as needed.

OPM

To: The Honorable Beth F. Cobert
Acting Director
U.S. Office of Personnel Management

From: Rep. Jason Chaffetz
Chairman

February 25, 2016 Committee on Oversight and Government Reform:

"Security Clearance Reform: The Performance Accountability Council's Path Forward."

Please reply by March 22, 2016 with responses to the following questions and requests:

1. **What is your proposed timeline for meeting the recommendations from the 120 day review of the security clearance process?**

   The 120 day review resulted in a number of recommendations in three main categories that span five years, many of which have been completed, some we are in the process of answering and some we will answer in the future. For example, we completed a number of actions to improve enterprise operations, including recomposing the Performance Accountability Council (PAC), establishing a PAC Program Management Office, founding an Enterprise Investment Board, and creating the Security, Suitability, and Credentialing (SSC) Line of Business (SSCLOB). Measures completed to reduce inherent risk in SSC processes included reducing the total population of clearance holders by 18%, formulating and issuing government-wide Quality Assessment Standards, and issuing guidance to all agencies mandating the use of the OPM supplemental standards for issuance of Personal Identity Verification (PIV) credentials. We have taken several significant steps to increase the availability of critical information, including instituting a Records Access Task Force study and issuing its findings, greatly expanding Continuous Evaluation (CE) pilots, and implementing Tiers One, Two, and Three of the revised Federal Investigative Standards (FIS) on schedule with the FIS Implementation Plan.

   The SSC reform partners (OMB, DoD, DNI, OPM, and the PAC) are continuing progress on a number of objectives that we expect to accomplish in the near term, including crafting an Enterprise Information Technology Strategy and associated implementation plan, expansion of social media pilots and issuance of a government-wide social media policy, implementation of initial operating capability of Tiers Four and Five of the FIS, and development of a government wide tool for agencies to report quality assessments of investigative quality. The Administration's Insider Threat and Security Clearance Reform (ITSCR) Cross-Agency Priority (CAP) Goal tracks and monitors progress on the Suitability and Security Processes Review recommendations and other ongoing reform effort initiatives. Progress updates on the ITSCR CAP Goal activities are publicly available on www.performance.gov.

2. **Please explain how NBIB impacts OPM and DOD Federal Information Technology Reform Act (FITARA) compliance obligations. Will NBIB's IT systems comply with FITARA requirements?**

   The IT systems for NBIB will comply with all appropriate IT statutes and regulations including FITARA. As we begin system design, DOD and OPM are working together to designate proper roles and responsibilities with respect to this compliance.

3. **Will contracts relating to IT security at NBIB or interim contracts relating to IT security at FIS include new provisions on access and information sharing? If so, what is the status of those new provisions?**

   OPM is in the process of updating the security provisions that will be included in its contracts, including requirements under NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organization,* and continues to keep them current with best practices and emerging threats. Recently released Requests for Proposals (RFPs) for Federal Investigative Service (FIS) Investigations Fieldwork, Investigations Support Services, and Central Records Unit Services include the updated provisions. OPM consulted with DOD on the content of these provisions in advance of releasing these RFPs, a practice OPM expects to continue.

   For existing contracts, OPM is taking a risk-based approach, identifying those (e.g., those for external applications containing personally identifiable information) which included earlier versions of the IT provisions, and will be prioritizing modifications to those higher risk contracts.

4. **For security clearance periodic reinvestigations that took place in 2015, please indicate what percentage of reinvestigations were completed:**
   a. **Between five and six years after the most recent previous reinvestigation or initial investigation;**
   b. **Between six and seven years after the most recent previous reinvestigation or initial investigation;**
   c. **Between seven and eight years after the most recent previous reinvestigation or initial investigation;**
   d. **Between eight and nine years after the most recent previous reinvestigation or initial investigation;**
   e. **Between nine years and ten years after the most recent previous reinvestigation or initial investigation; and**
   f. **Over ten years after the most recent previous reinvestigation or initial investigation.**

Agencies are responsible for initiating reinvestigation requests within the prescribed timeframes. Note that, currently, secret clearances have a reinvestigation requirement after 10 years so based on the general scope of the question the below table shows data for TS clearances. The below table shows that approximately 83% of investigations for TS clearance were submitted within six

years of the previous SSBI or reinvestigation, and 90% were submitted within seven years. FIS does not have data for a certain percentage of cases where the initial investigation was completed by another entity.

National Security Reinvestigations With A Previous Investigation (SSBI or Reinvestigation)
10/01/2014 through 09/30/2015

		Reinvestigations Initiated within Time Frames:							
Total Reinvestigations Closed in FY15	Total Previous SSBI and/or Reinvestigations	0-5 years	5-6 years	6-7 years	7-8 years	8-9 years	9-10 years	over 10 years	No Previous SSBI/ Reinvestigation
91,478	85,426	38,298	37,478	6,488	1,699	514	366	583	6,052*
Percentages	93.39%	41.87%	40.97%	7.09%	1.86%	0.56%	0.40%	0.64%	6.61%

*Indicates prior investigation completed by another Investigative Service Provider other than OPM

To: The Honorable Beth F. Cobert
Acting Director
U.S. Office of Personnel Management

From: Rep. Steve Russell (OK-05)
Member of Congress

February 25, 2016 Committee on Oversight and Government Reform:

"Security Clearance Reform: The Performance Accountability Council's Path Forward."

Please reply by March 22, 2016 with responses to the following questions and requests:

Congress remains very concerned over the Executive Branch's ability to oversee the security clearance process, not only guaranteeing that only trusted persons have access to classified information but that the process can identify insider threats and adequately safeguard personal information. The Edward Snowden leaks, the Navy Yard shooting, and OPM data breach offer case in point. Although the establishment of the National Background Investigative Bureau (NBIB) is well intentioned, it fails to address some of the fundamental problems with the current security clearance architecture. Further, the Office of Personnel Management claims this new organization will "modernize the process, leverage the Department of Defense's cyber expertise, and boost operational flexibility." However, no mention is made of leveraging the capabilities and best practices from relevant industry thought leaders:

1. **Is NBIB envisioned as a consolidation of existing capabilities under one authority or is this an opportunity to build a purpose-driven system from the ground up?**

   The creation of NBIB provides us the opportunity to make important operational and structural changes to better meet its mission to provide effective, efficient, and secure background investigations for the Federal Government. These changes will maximize the use of existing capabilities and add important additional capabilities to strengthen how the Federal government preforms background investigations.

   Importantly, the Department of Defense, with its unique national security perspective and cybersecurity expertise, will design, build, secure, and operate the NBIB's investigative IT systems in coordination with the NBIB.

   The NBIB will receive dedicated support in key operational areas, and we will bring in additional talent with a focus on national security expertise as we do so. The NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up

and new IT systems are developed. The head of the NBIB will be elevated to become a full member of the Performance Accountability Council (PAC) with the aim of synchronizing both the policy and operational functions related to background investigations.

2. What best practices are you leveraging from relevant industry thought and technology leaders?

The interagency team who developed the 90-day recommendations consulted with industry stakeholders in the development of the recommendations, and will continue to work closely with industry experts and our interagency partners including DHS and OMB as NBIB's systems are designed and built. Outreach to industry technology leaders will be an essential input our work moving forward. The Transition Team, OPM, and DOD are working with the technology industry in four main areas:

- security; embedding security principles in all phases of the systems development lifecycle and operations to align with the Cyber National Action Plan ;
- data and data providers; identifying valuable data sources, and also to re-thinking and re-designing how data is collected, aggregated, used and purged in the background investigative process;
- application development; building applications that users want, are intuitive, and are achieved in more real time;
- lifecycle flexibility; hosting and maintaining systems in a modern technology environment that is consistent with private sector cloud offerings.

The PAC's interagency Security, Suitability, and Credentialing Line of Business is currently developing an Enterprise IT Strategy that will incorporate modern industry best practices, which will be leveraged during implementation of that Strategy over the next five years. This includes, for example:

- incorporating the U.S. Digital Services Playbook, which adopts private sector best practices and standards for the design and delivery of new or modified SSC IT systems and applications;
- acquiring new IT systems by leveraging an agile procurement approach supported by the TechFAR;
- adopting cloud-based services, where appropriate, as outlined in the Federal Cloud Computing Strategy; and
- focusing the effort on providing minimum viable product (i.e. meeting business needs with the smallest, fastest investment), which is the practice found at the best technology companies in the private sector.

3. **What successes and challenges are you facing with implementing a Continuous Evaluation of Cleared Personnel program?**

The development and implementation timeline for a government-wide Continuous Evaluation (CE) Program is part of the larger, on-going personnel security reform efforts. The ODNI CE Program is developing policy, standards, and guidance for the implementation of CE for the most sensitive populations across the executive branch, in support of the implementation of the 2012 Federal Investigative Standards (FIS). Further, in 2014, DOD initiated a CE concept demonstration on approximately 100,000 cleared military, DOD civilian, and contractor personnel using a limited set of trusted commercial and government data sources. Late last year DOD expanded their CE pilot capability to include 225,000 DOD government and contractor personnel. As such, I defer to ODNI and DOD for a response to this question.

4. **Are you facing any policy or legislative roadblocks in implementing a Continuous Evaluation of Cleared Personnel program?**

Given the work that ODNI and DOD have done in this area, I defer to them for a response to this question.

To: The Honorable Beth F. Cobert
Acting Director
U.S. Office of Personnel Management

From: Rep. Elijah Cummings
Ranking Member

February 25, 2016 Committee on Oversight and Government Reform:

"Security Clearance Reform: The Performance Accountability Council's Path Forward."

Please reply by March 22, 2016 with responses to the following questions and requests:

1. **According to testimony you provided during the February 25 hearing, Anthem Inc. is contractually required to report network breaches to OPM and did so after a February 2015 cyberattack resulted in the loss of personally identifiable information (PII) of nearly 80 million people.**

In response to questions of whether a similar requirement exists for network compromises to be reported to the United States Computer Emergency Readiness Team (US-CERT), you stated:

> **"I don't believe that the contract requires them to report to US-CERT, but as we're looking at the new contracts and as we're working with all of our health insurance partners, that is one of the options we are exploring."**

In response to the committee's concerns regarding the lack of such a requirement and whether a requirement should exist, you stated:

> **"Improving our ability to work with our contractors on cyber security is a key priority for us at OPM and I know it is across the executive branch. We have been reviewing the clauses in our contracts and working to ensure that we can make, that those have the provisions that we need going forward ... those are the -- well, the kinds of clauses we were looking to implement going forward."**

a. **Please identify and provide copies of the contractual clauses OPM requires for each of its contractors detailing the responsibilities of those contractors to report cyber breaches to the agency. In identifying the requested clauses for the Committee, the information that should be provided should include the following:**
   a. **The name of the contractor to whom the contract relates;**
   b. **To whom the reports must be made;**

c. **What information must be reported;**
d. **How long after a breach is discovered must the report be made;**
e. **Any immunity from liability provided to the contractor for reporting the breach; and**
f. **The consequences of non-compliance with any reporting requirements.**

Improving our ability to work with our contractors on cyber security is a priority for OPM. We have completed our review of the contract clauses previously used by OPM in the past for our largest IT contracts in addition to starting a comprehensive review of our existing IT contracts. Attachment 1 includes the clauses used by OPM since 2012 in contracts that allow or require access to PII, and/or where performance requires access to OPM IT systems, necessitating notification in case of a security incident. OPM has completed an update to the IT contract clauses in 2016 (see Attachment 2) to strengthen the reporting requirements by contractors in the event of a security breach. The 2016 clauses more specifically address the requirements for contractors to notify OPM of all IT security incidents, to whom the reports must be made, and when the report must be made as well as tighter timelines for reporting for future OPM IT contracts.

IT notification requirements for Carriers under the Federal Employee Health Benefits (FEHB) Program are conveyed differently. Carriers must report all Significant Events to their OPM Contracting Officer. Significant Events are defined in FEHB Program regulations at FEHBAR 1652-70 (JUL 2005) and in every FEHB Program contract. To further clarify our expectations with regard to reporting Significant Events that involve a breach of Carrier IT systems under this clause, we released Carrier Letter 2015-04 in March 2015, which is shown at Attachment 3.

In addition, OPM has formed an ongoing FEHB Carrier IT Security Workgroup to ensure FEHB Carriers' practices remain complete and effective with regard to reporting data breaches. The Department of Homeland Security and the Department of Health and Human Services are participating with us in our workgroup and collaborating with us as we work to ensure our requirements are up to date with all legislation and regulations regarding IT security and reporting including the recently passed Cybersecurity Information Sharing Act of 2015.

The FEHB Program contract clause that relates to breaches of OPM IT systems (Attachment 4) also requires reporting within 30 minutes of the risk of breach regardless of the time or day of the week.

The new contract clauses we are finalizing applying to most other large OPM IT contracts also expand OPM's ability to access contractors' IT systems to perform inspections and forensic analysis by US-CERT or any other agency involved in remediation in the event of a cyber breach. Both section 1752.239-86 in the original clauses, as well as section 1752.224-72 of the new clauses, provide for logical and physical access to the contractors' facilities, records and databases. The new clauses

expand OPM's ability to access the contractors' systems for purposes of inspection and forensic analysis and not just to assess and monitor contractor systems and infrastructure for OPM contracts that use contractor IT systems.

OPM is making sure we have the provisions we need going forward. OPM has already incorporated the new clauses in three major Requests for Proposals (RFPs) recently released for Federal Investigative Fieldwork Services, Investigations Support Services, and Central Records Unit procurements. OPM is also developing interim guidance to be issued in the near future to require the incorporation of the revised contract clauses into new solicitations and existing contracts, as appropriate, to assure the maximum level of assurance that our data is secure and that we have the ability to respond and remediate in the event of a cyber attack. This interim guidance will then be substituted by formal policy institutionalizing the new clauses as mandatory at OPM for future contracts, as applicable. As new legislation is enacted, such as the Cybersecurity Information Sharing Act, OPM will incorporate additional provisions as needed.

The clauses cited above do not mention immunity from liability for reporting the breach. At the Contracting Officer's discretion, non-compliance with the contractual requirements may be grounds for a variety of administrative remedies including, but not limited to, documenting in the contractor's performance assessment, issuance of letters of concern or cure notices, not exercising future contract options, and/or even termination of the contract depending on the specific circumstances and impacts.

2. **Please identify and provide copies of contractual clauses in OPM contracts that are currently in effect, or that are in the process of being proposed, that would require contractors to cooperate with US-CERT and any other federal agency involved in remediation, in the event of a cyber breach.**

See the response to question 1 above.

Attachment 1

NOTE: Clauses provided for below are not included in full text. Only the sections applicable to the response are provided.

Original Clauses (2012)

1752.224-70 Protecting Personally Identifiable Information (Nov 2012)

....

(f) IT Security Incident and PII Breach Protection and Notification

All security incidents that involve OPM information or information systems must be reported to the OPM Situation Room. Contractors must also report incidents to the OPM Contracting Officer. This reporting must occur immediately upon discovery of the incident. Incidents and breaches must be reported, even if it is believed the breach is limited, small, or insignificant. OPM's IT security experts will determine when a breach needs additional focus and attention. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail.

1. OPM contractors must report a breach or potential security breach to the OPM Situation Room at: sitroom@opm.gov, (202) 418-0111, Fax (202) 606-0624.
2. When notifying the Situation Room, copy the Contracting Officer.
3. If you have questions regarding these procedures, contact the Contracting Officer.

1752.239-86 Contractor System Oversight/Compliance (Nov 2012)

....

(b) The Contractor shall support the OPM in its efforts to assess and monitor the contactor systems and infrastructure. The contractor shall provide logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases upon request. The contractor will be expected to perform automated scans and continuous monitoring activities which may include, but not limited to, authenticated and unauthenticated scans of networks, operating systems, applications, and databases and provide the results of the scans to OPM or allow OPM personnel to run the scans directly.

Attachment 2

NOTE: Clauses provided for below are not included in full text. Only the sections applicable to the response are provided.

New Clauses (2016)

1752.224-72 Access to Contractor Information Technology (IT) Systems (Dec 2015)

During the period of performance of the contract and throughout any contract close-out period, the Contractor must provide OPM, or its designate, with immediate access to all IT systems used by the Contractor to support the performance of the contract for the purpose of inspection and forensic analysis in the event of an Information Security Incident (ISI).

(End of Clause)

1752.224-77 Information Security Incidents (ISI) (Dec 2015)

a. ISI Reporting Activities

(1) Contractors must report any and all ISI involving OPM Information to the OPM Situation Room (SITRoom) at SITROOM@OPM.GOV, voice: 202-418-0111, fax: 202-606-0624. The SITRoom is available 24 hours per day, 365 days per year.

(2) Contractors must report any and all ISI involving information technology (IT) systems and Controlled Unclassified Information (CUI) immediately upon becoming aware of the ISI but no later than 30 minutes after becoming aware of the ISI, regardless of day or time; regardless of internal investigation, evaluation, or confirmation of procedures or activities; and regardless of whether the ISI is suspected, known, or determined to involve IT systems operated in support of this contract.

(3) Contractors reporting an ISI to the SITRoom by email, phone, or fax must copy the Contracting Officer (CO) or Contracting Officer's Representative (COR) if possible; but if not, must notify the CO or COR immediately after reporting to the SITRoom.

(4) When reporting an ISI to the SITRoom by email:

(a) Do not include any CUI in the subject or body of any email;

(b) Use FIPS 140-2 compliant encryption methods to protect CUI to be included as an email attachment, and do not include passwords in the same email as the encrypted attachment; and

(c) Provide any supplementary information or reports related to a previously reported incident directly to the OPM SITRoom with the following text in the subject line of the email: "Supplementary Information / Report related to previously reported incident # [insert number]."

b. ISI Review and Response Activities

(1) The Contractor must provide full access and cooperation for all activities determined by CO or COR to be required to ensure an effective review and response to protect OPM's Information and Information Systems operated in support of this contract.

(2) The Contractor must promptly respond to all requests by the CO or COR for ISI and system-related information, including but not limited to disk images, log files, event information, and any other information determined by OPM to be required for a rapid but comprehensive technical and forensic review.

(3) OPM, at its sole discretion, may obtain the assistance of Federal agencies and/or third party firms to aid in ISI Review and Response activities.

c. ISI Determination Activities

(1) The Contractor must not make any determinations related to an ISI associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract, including determinations related to notification of affected individuals and/or Federal agencies (except reporting criminal activity to Law Enforcement Organizations) and offering of services, such as credit monitoring.

(2) The Contractor must not conduct any internal ISI-related review or response activities that could modify or eliminate any existing technical configuration or information or forensic technical evidence existing at the time of the ISI without approval from the OPM Chief Information Officer (CIO) through the CO or COR.

(3) All determinations related to an ISI associated with Information Systems or Information maintained by the Contractor in support of the activities authorized by this contract will be made only by the OPM CIO through the CO or COR.

(4) The Contractor must report criminal activity to Law Enforcement Organizations upon becoming aware of such activity.

(End of Clause)

Attachment 3

NOTE: Clauses provided for below are not included in full text. Only the sections applicable to the response are provided.

FEHBP Carrier Letter

See *https://www.opm.gov/healthcare-insurance/healthcare/carriers/2015/2015-04.pdf*

Attachment 4

NOTE: Clauses provided for below are not included in full text. Only the sections applicable to the response are provided.

FEHBP Breach Notification Clause

SECTION 1.35

PROCEDURES FOR REPORTING A LETTER OF CREDIT SYSTEM SECURITY BREACH (JAN 2013)

(a) A breach of data, system access, etc. includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of information whether physical or electronic. As an agency, OPM is required to immediately report all potential security and data breaches -- whether they involve paper documents or electronic information. In order to meet this responsibility, OPM has established a new internal procedure for reporting the loss or possible compromise of any data, and this clause conforms to that procedure.

(b) OPM Carriers must report any breach or potential breach to the OPM Situation Room and the Contracting Officer within 30 minutes of becoming aware of the risk – regardless of the time or day of the week. Breaches should be reported, even if it is believed the breach is limited, small, or insignificant. OPM's IT security experts, who will determine when a breach needs additional focus and attention. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail.

(1) OPM Carriers must report a breach or potential security breach to the OPM Situation Room at: sitroom@opm.gov, (202) 418-0111, Fax (202) 606-0624.

(2) When notifying the Situation Room, please copy the Contracting Officer.

(3) To get help with WinZip, please contact the OPM Help Desk at: helpdesk@opm.gov, (202) 606-4927, TTY (202) 606-1295.

(4) If you have questions regarding these procedures, contact the Contracting Officer.

FEHB Program Carrier Letter
All FEHB Carriers

U.S. Office of Personnel Management
Healthcare and Insurance

Letter No. 2015-04 **Date: 03/23/2015**

Fee-for-Service [4] Experience-rated HMO [4] Community-rated [3]

SUBJECT: Notification of Data Breach

The purpose of this communication is to provide you with updated information concerning the importance of data security and notification to OPM.

Any breach of security in Federal Employees Health Benefits (FEHB) enrollee data is considered a significant event as defined in Section 1.10 Notice of Significant Events (FEHBAR 1652.222-70) of the FEHB Standard Contracts. This includes any breach of security in a carrier IT network that may potentially affect FEHB enrollee data. Although the contracts require notification of a significant event within 10 working days after the carrier becomes aware of it, due to privacy concerns and the potential impact on FEHB enrollees, we require notice to OPM immediately if you know or suspect that a breach has occurred. For any security breach or potential breach, immediate notification means that carriers will notify OPM within 30 minutes of becoming aware of the risk, regardless of the time or day of the week. This procedure is consistent with the provisions of the standard FEHB carrier contract applicable to reporting a Letter of Credit security breach. OPM has issued previous carrier letters on this topic – please reference Carrier Letter 2007-21, dated June 22, 2007 and Carrier Letter 2010-14, dated May 25, 2010.

A breach of data, system access, etc. includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of information whether physical or electronic. As an agency, OPM is required to immediately report all potential security and data breaches -- whether they involve paper documents or electronic information. In order to ensure FEHB carriers also comply with this requirement, we are issuing the following guidance.

FEHB carriers, by contract, must report any breach, suspected breach, or potential breach to OPM. We are updating our guidance to notify you that this report should be made to the **OPM Situation Room** and to the Contracting Officer immediately upon becoming aware of the risk. A suspected breach, potential breach or breach must be reported, even if it is believed the breach is limited, small, or insignificant. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail. Below are further instructions.

1. OPM carriers must report a breach, suspected breach, or potential security breach to the OPM Situation Room at: sitroom@opm.gov, (202) 418-0111, Fax (202) 606-0624.
2. When notifying the OPM Situation Room, please copy your Contracting Officer.

3. If you need assistance with WinZip, please contact the OPM Help Desk at: helpdesk@opm.gov, (202) 606-4927, TTY (202) 606-1295.
4. If you have questions regarding these procedures, please contact your Contracting Officer.

In addition, FEHB carriers, by contract, are required to cooperate with OPM's Office of the Inspector General (OIG) in their evaluation of your organizations' ability to protect the confidentiality, availability, and integrity of sensitive or mission-critical data. The OIG conducts independent evaluations to determine whether organizations have the controls in place to ensure its computer systems are securely configured and up-to-date. These evaluations involve the use of OIG hardware and/or software to conduct vulnerability scans and configuration compliance audits against a sample of the carrier's computer systems. The data obtained during the scans allows the auditors to form an opinion as to whether the organization has sufficient controls in place to protect sensitive or mission critical data. These evaluations are conducted in accordance with rules of engagement that provide assurance that the audit will not have a negative impact to the IT systems involved in the review. We expect all FEHB carriers to provide prompt and complete cooperation to allow the OIG to carry out its responsibilities in conducting its audits.

If you have any questions concerning the guidance in this Carrier Letter, please contact your Contracting Officer.

Sincerely,

John O'Brien
Director
Healthcare and Insurance

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
DIRECTOR OF LEGISLATIVE AFFAIRS
WASHINGTON, DC 20511

MAY 12 2016

The Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

The enclosed document responds to Questions for the Record following the 25 February 2016 hearing regarding the establishment of the National Background and Investigations Bureau as well as Security Clearance Reform.

Please do not hesitate to contact my office at (703) 275-2474 if you require further assistance regarding this or any other matter.

Sincerely,

Deirdre M. Walsh

Deirdre M. Walsh

Enclosure:
Responses to Questions for the Record from the 25 February 2016 Hearing before the House Oversight and Government Reform Committee

cc:
The Honorable Devin Nunes
The Honorable Adam B. Schiff

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 1: Which agencies overseen by ODNI still lack a continuous evaluation program in accordance with ODNI guidance?

Answer: The Office of the Director of National Intelligence (ODNI), through the National Counterintelligence and Security Center (NCSC), continues to work with many agencies across the executive branch to leverage each other's capabilities in order to collectively meet the September 30, 2017 deadline for fully operational Continuous Evaluation (CE) programs. There are many agencies conducting CE-like activities, which include checks of records sources for a fully operational CE program that meets the standard requirements. For example, the Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, and National Geospatial-Intelligence Agency have access to multiple internal and external records sources and use them to conduct periodic checks as part of their CE-like activities and Executive Branch agencies, such as the Department of Defense (DoD) and Department of State, have conducted pilots to explore the effectiveness of on-going automated records checks as part of their CE-like activities. However, at this time, no single agency utilizes all of the required data sources in order to implement a fully operational CE program as established by the ODNI.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 2: What is the current status of efforts to incorporate social media into the security clearance process?

Answer: Multiple agencies, including the DoD have conducted social media pilots to gain insight into the issues and to understand the benefits associated with conducting a social media check as part of the personnel security vetting process. Continued analysis of these pilots' results will guide the way forward as well as identify areas requiring additional research. Additionally, the DNI, in his role as the Security Executive Agent, directed the drafting of a Security Executive Agent Directive (SEAD 5) on Social Media, to provide guidance on the use of social media checks in the personnel security vetting process. After extensive review, Director Clapper has approved SEAD 5. A notification was provided to Congressional committees of jurisdiction on May 12.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 3: For security clearance periodic reinvestigations that took place in 2015, please indicate what percentage of reinvestigations were completed:

a) Between five and six years after the most recent previous reinvestigation or initial investigation;
b) Between six and seven years after the most recent previous reinvestigation or initial investigation;
c) Between seven and eight years after the most recent previous reinvestigation or initial investigation;
d) Between eight and nine years after the most recent previous reinvestigation or initial investigation;
e) Between nine years and ten years after the most recent previous reinvestigation or initial investigation; and
f) Over ten years after the most recent previous reinvestigation or initial investigation.

Answer: The requested data on the age of the previous background investigation being updated is not collected. The ODNI collects and reports metrics on investigative production and timeliness for periodic reinvestigations (PRs). Data is also collected regarding the size of the national security population with out-of-scope PRs. The collection and reporting is done using the total number of completed or overdue PRs, by agency, at the end of each fiscal quarter.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 4: Is NBIB envisioned as a consolidation of existing capabilities under one authority or is this an opportunity to build a purpose-driven system from the ground up?

Answer: The NBIB is an excellent opportunity to build a new purpose-driven system from the ground up. NCSC supports the use of DoD's IT systems as a foundation for the restructuring and believe they will provide this new entity with exceptional capabilities.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 5: What best practices are you leveraging from relevant industry thought and technology leaders?

Answer: The ODNI has regularly studied the best practices of industry and technology leaders to improve the security clearance processes. For example, we are adopting new principles of business process improvement, automation, streamlining, redundancy elimination, and program management. Additionally, we conduct monthly meetings with an industry roundtable, consisting of counterintelligence and security personnel from cleared industry, who provide advice on a wide range of security issues.

In 2013, ODNI NCSC Special Security Directorate personnel repeatedly met with Industrial Security Working Group (ISWG) and the Intelligence and National Security Alliance (INSA) members about expanding industry access to Scattered Castles security clearance data. Together they suggested potential changes to Scattered Castles which were then presented as a formal change to Scattered Castles User Roles for Industry personnel. The Scattered Castles Executive Steering Group (SCESG) then approved the new user role specifically for Industry Users.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 6: What successes and challenges are you facing with implementing a Continuous Evaluation of Cleared Personnel program?

Answer: The ODNI, through the NCSC, has successfully coordinated with Executive Branch agencies to address CE implementation. Specifically, through an interagency working group, stakeholders from across the executive branch have been collaborating on recommendations for the development of standards and guidance for programmatic and technical implementation of CE. ODNI's CE Program continues to work with the PAC PMO, DoD, and OPM, as well as other partners to leverage lessons learned and best practices from on-going automated records checks pilots and CE-like efforts currently underway.

One challenge is the ability to gain access to the required data sources for CE. The ODNI CE Program continues to work with government data providers to establish necessary agreements and technical connectivity to support efficient negotiation and acquisition of critical data and to share this information with our CE stakeholders. Additionally, the technical complexity of building cross domain solutions that allow robust communications/interactions between classified and unclassified environments in a secure, cost efficient manner, remains a challenge. Despite these issues, the ODNI will work with the NBIB and interagency partners to establish a CE program.

Hearing Date: 25 February 2016
Committee: HOGR
Witnesses: William Evanina
Beth Cobert
Terry Halverson
Tony Scott
Info Current as of: 12 May 2016

Question 7: Are you facing any policy or legislative roadblocks in implementing a Continuous Evaluation of Cleared Personnel program?

Answer: The recent amendment of 5 USC 9101, for the inclusion of criminal history record information in national security investigations by authorized investigative service providers, addressed a significant obstacle to the implementation of CE. However, the lack of funds to support access to criminal history records held by the FBI for national security investigative purposes remains a challenge for agencies seeking to use this data for personnel security investigative activities, including CE. Additionally, the ODNI CE program faces challenges in providing funding to non-IC agencies to support technical connectivity to, and integration with, the developing ODNI CE system.

OMB

1. Why have social media checks not become standard practice in the security clearance process?

Response:

The Office of the Director of National Intelligence (ODNI) in its role as the Security Executive Agent has developed a social media policy that has undergone extensive coordination with relevant department and agency officials, including the agencies with significant national security missions and the Federal CIO Privacy Committee. The goal has been to ensure that the policy strikes the right balance between national security and civil liberties, and that appropriate privacy protections were included, especially with respect to validating and adjudicating adverse information that is discovered and collecting information about third parties.

The ODNI took a deliberative approach in developing its policy. It was informed by social media pilots conducted by multiple agencies, including the Department of Defense (DoD), giving insight into the issues, costs, and benefits associated with conducting a social media check as part of the personnel security vetting process. Continued analysis of the pilot results will guide the way forward and identify areas requiring additional research.

This policy is being finalized and, once signed by the Director of National Intelligence (DNI), will be issued.

2. Congress remains very concerned over the Executive Branch's ability to oversee the security clearance process, not only guaranteeing that only trusted persons have access to classified information but that the process can identify insider threats and adequately safeguard personal information. The Edward Snowden leaks, the Navy Yard shooting, and OPM data breach offer case in point. Although the establishment of the National Background Investigative Bureau (NBIB) is well intentioned, it fails to address some of the fundamental problems with the current security clearance architecture. Further, the Office of Personnel Management claims this new organization will "modernize the process, leverage the Department of Defense's cyber expertise, and boost operational flexibility." However, no mention is made of leveraging the capabilities and best practices from relevant industry thought leaders:

2(a) Is NBIB envisioned as a consolidation of existing capabilities under one authority or is this an opportunity to build a purpose-driven system from the ground up?

Response:

The NBIB will assume the existing OPM Federal Investigative Services (FIS) personnel and support structure, and will be responsible for the existing FIS mission to provide effective, efficient, and secure background investigations for the Federal Government. While several existing FIS capabilities will be absorbed into the new organization, its information technology capabilities will be purpose-built for that mission. An initial milestone for the transition to the NBIB is to develop a sunset/migration schedule in place for all OPM FIS IT systems.

NBIB will also operate under a new structure. NBIB will report to the OPM Director, but unlike

the previous structure, DOD will assume responsibility for the design, development, security, and operation of the background investigations IT systems for the new entity. The head of NBIB will be Presidentially-appointed and a full member of the Performance Accountability Council (PAC). NBIB will receive policy direction and guidance from and be accountable to the PAC and its customer agencies for providing continuous improvements to the investigative process; and NBIB will have a dedicated senior privacy official to advance privacy-by-design as the new entity is stood up and new IT systems are developed. A cadre of interagency personnel will help stand up the new entity and be part of its ongoing management.

2(b) What best practices are you leveraging from relevant industry thought and technology leaders?

Response:

The Administration, through the interagency PAC, and in consultation with government and industry subject matter experts, is currently developing an Enterprise IT Strategy that will incorporate modern industry best practices, which will be leveraged during implementation of that Strategy over the next five years. This includes, for example:

- embedding security principles in all phases of the systems development lifecycle and operations to align with the Cybersecurity National Action Plan;
- incorporating the U.S. Digital Services Playbook, which adopts private sector best practices and standards for the design and delivery of new or modified SSC IT systems and applications;
- acquiring new IT systems by leveraging an agile procurement approach supported by the TechFAR; and
- adopting cloud-based services, where appropriate, as outlined in the Federal Cloud Computing Strategy.

2(c) What successes and challenges are you facing with implementing a Continuous Evaluation of Cleared Personnel program?

Response:

The development and implementation timeline for a government-wide Continuous Evaluation (CE) Program is part of the larger, on-going personnel security reform efforts, and not in response to any particular event, such as the NSA disclosures or the Navy Yard shooting.

The ODNI CE Program is developing policy, standards, and guidance for the implementation of CE for the most sensitive populations across the executive branch, in support of the implementation of the 2012 Federal Investigative Standards. The ODNI will soon disseminate implementation guidance to Executive Branch agencies requesting that they respond to the DNI with their plans for CE implementation.

In its role as the Security Executive Agent, the ODNI continues progress on developing a government-wide CE capability for Federal departments and agencies, including the Intelligence Community, to establish a process for more frequent background reviews of our highest risk

populations. The ODNI is working with their interagency partners to access new sources of electronic and automated data to support more robust capabilities for CE.

In accordance with the Federal Investigative Standards, the initial target enrollment for CE is a portion of the Tier 5 (Top Secret-level) population. Enrollment may be expanded to include a substantially larger percentage of the Tier 5 population and the Tier 3 (Secret-level) population.

Further, in 2014, DoD initiated a CE concept demonstration on approximately 100,000 cleared military, DoD civilian, and contractor personnel using a limited set of trusted commercial and government data sources. Late last year DoD expanded their CE pilot capability to include 225,000 DoD government and contractor personnel. .

To date, the challenges encountered during the design, development, and testing of the ODNI's CE System (CES) or the DoD's concept demonstration have not been insurmountable nor unusual.

2(d) Are you facing any policy or legislative roadblocks in implementing a Continuous Evaluation of Cleared Personnel program?

Response:

The Administration is in the process of evaluating whether any investigative capabilities, including continuous evaluation, will require some ancillary legislative changes, and will propose those targeted changes once determined. Likewise, as part of the process for standing up the NBIB, the interagency PAC is evaluating whether this will require changes to legislative or Executive branch-wide or agency-specific policy.

○