IMPROVING SECURITY AND EFFICIENCY AT OPM AND THE NATIONAL BACKGROUND INVESTIGATIONS BUREAU

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

FEBRUARY 2, 2017

Serial No. 115–12

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

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

U.S. GOVERNMENT PUBLISHING OFFICE

26–358 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 J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Trey Gowdy, South Carolina
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan

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
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland

JONATHAN SKLADANY, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
JULIE DUNNE, *Senior Counsel*
MICHAEL FLYNN, *Counsel*
SHARON CASEY, *Deputy Chief Clerk*
David Rapallo, *Minority Staff Director*

CONTENTS

IMPROVING SECURITY AND EFFICIENCY AT OPM AND THE NATIONAL BACKGROUND INVESTIGATIONS BUREAU

Thursday, February 2, 2017

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

The committee met, pursuant to call, at 9:02 a.m., in Room 2154, Rayburn House Office Building, Hon. Jason Chaffetz [chairman of the committee] presiding.

Present: Representatives Chaffetz, Jordan, Amash, Massie, Meadows, DeSantis, Ross, Blum, Hice, Grothman, Hurd, Palmer, Comer, Mitchell, Cummings, Maloney, Lynch, Connolly, Kelly, Lawrence, Plaskett, Demings, Krishnamoorthi, and Raskin.

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

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

I appreciate you all being here. We have a very important hearing. We have a number of members that, I'm sure, will be here but will be a little bit late. There is the National Prayer Breakfast, and getting across town at this time of day is a very difficult task, so——

But, nevertheless, I'm glad to have you here and look forward to this important hearing.

Two years ago, the Office of Personnel Management suffered one of the most damaging data breaches in the history of the Federal Government. This went on for some time, and there are still additional details that need to be learned.

But the counterintelligence value of the data that was stolen will last for an untold amount of time, a generation or so. So it troubles me to hear reports that maybe some of the things that led to this haven't necessarily been changed at the Office of Personnel Management.

We have a number of questions that I think we need to explore. For example, are legacy systems still in use for backup investigations? Is OPM employing good cybersecurity practices such as dual factor authentication and network segmentation? What is the plan to transition all of OPM's systems off this legacy technology? When will OPM stop using unsecured and vulnerable legacy technologies such as Cobalt and start using maybe some modernized solutions that can be put on the cloud?

How is OPM protecting the inside of the network and not just building the cyberwalls higher? Will OPM adopt a zero-trust model as part of their cybersecurity strategy? You can't steal what you can't access, and a zero-trust model makes life much harder for the hackers. These are some of the questions we'll continue to ask and explore.

We said it in the committee's data breach report, and I'll say it again, chief information officers matter. They really do matter. That's why we have two of them on the panel today. Federal agencies, particularly CIOs, must recognize their positions are on the frontline of defense against these cyber attacks. And as the government, we're on notice. Leadership at the Federal agencies must be vigilant about the ever-present national security threats targeting their IT systems. And especially in OPM's case where the IT systems are protecting some of the most vulnerable information held by the Federal Government.

The National Background Investigation Bureau, also known as NBIB, N–B–I–B, was partly born from the failures at the Office of Personnel Management. When OPM last testified before the committee, in February of 2016, the NBIB had just been announced. During the hearing, questions were raised about the accountability and how this new organization would operate given the split responsibilities with OPM overseeing the NBIB and the Department of Defense overseeing the IT security of the NBIB.

Today, we'd like answers to those questions and assurances that we're moving in the right direction and also, as to when the new organization will be fully operational with a secure IT environment.

Was the creation of the NBIB simply a rebranding effort, or does the NBIB represent real change? At our last hearing, we talked about how the many security clearance processes failed to check social media information of the applicants. The day before our follow-up hearing in May of 2016, the director of National Intelligence issued a new policy permitting the collection of publicly available social media information in certain cases. We'd like to understand how this policy is being implemented and if it is effective.

Finally, the clearance process seems to be getting worse while the reform process continues. My understanding is at least—based on an OPM management memo of October 2016, there's a backlog—at least then—there was a backlog of 569,000 cases. That's quite a list. It does beg the question as to why we have to have so many background checks, but where are we at in terms of the backlog? And why, despite all the reform activities, is the clearance process taking longer?

In fiscal year 2015, it took an average of 95 days to process a secret clearance and 179 days for a top secret clearance. In fiscal year 2016, it took an average of 166 days to process a secret clearance and 246 for a top secret clearance. That's quite a jump in the timeline that it takes in order to get there.

More than a decade ago, the security clearance data and processes were transferred from the Department of Defense to OPM, and now there's talk of transferring this process back to the Department of Defense. We also have the newly created NBIB where OPM and DOD have a shared responsibility. And we need to get

this right, make sure that we have stopped just moving the organizational boxes around.

As we continue our oversight of the transition of responsibilities from OPM to the NBIB, we need to continue to ask about the efficiency and making sure, at the end of the day, that we're protecting and securing the United States of America.

So there are a tremendous amount of number of people that are working on IT issues. We will have additional hearings and discuss that.

I personally do believe—and this is—at some point, I would like to draw this out from you—attracting and retaining IT professionals has got to be a challenge for the government. It's a challenge in the private sector. It's a challenge across the board.

I was fortunate enough to have a newly minted son-in-law, who is in the IT field. And the opportunities for him for employment were unbelievable. I've never seen anything like it, which is good as his father-in-law. That's a good thing.

But on a serious note, I do think we have to address, on the whole of government—not just this particular field, but the whole of government—how do we attract and retain IT professionals, because we do need so many of them, and there's so much vulnerability for the country as a whole.

So this is an important hearing, and I appreciate you being here. And now I'd like to recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman. I want to thank you for calling this hearing.

And as I listen to you talk about the IT people, Mr. Chairman, this is very important that we all let Federal employees know how important they are, and that we do everything in our power to provide them with the types of salaries and work security that they need. That's one of the things that would help to attract them and keep them.

Today's hearing is on the process our Nation uses to conduct background checks for Federal employees, who are seeking very important security clearances so they can have access to our most guarded secrets.

This hearing could not come at a more critical time. Yesterday, I sent a letter requesting a Pentagon investigation of the President's national security adviser, Lieutenant General Michael Flynn, for his potentially serious violation of the United States Constitution. I was joined by the ranking members of the committees on Armed Services, Judiciary, Homeland Security, Foreign Affairs, and Intelligence.

General Flynn has admitted that he received payment to appear at a gala in December of 2015 hosted by Russia Today, that country's State-sponsored propaganda outlet.

During that event, General Flynn dined with Russian President, Vladimir Putin. As our letter explains, the Department of Defense warns its retired officers that they may not accept any direct or indirect payment from foreign governments without congressional approval, because they continue to hold offices of trust under the emoluments clause of the United States Constitution.

On January 6, intelligence officials issued their report detailing Russia's attack on the United States to undermine our election.

This report concluded with high confidence that the goal was to, quote, "undermine public faith in the United States' democratic process," end of quote.

This report described as, quote, "The Kremlin's principle international propaganda outlet," end of quote. It explained—and I quote—that "The Kremlin's staff's RT and closely supervises RT's coverage recruiting people who can convey Russian's strategic messaging because of their ideological beliefs," end of quote.

It is extremely concerning that General Flynn chose to accept payment for appearing at an event hosted by the propaganda arm of the Russian Government at the same time that the country was engaged in an attack against this Nation in an effort to undermine our election. Something is wrong with that picture.

But it is even more concerning that General Flynn, who President Trump has now chosen to be his national security adviser, may have violated the Constitution in the process. We do not know how much General Flynn was paid for this event and for his dinner with President Putin, whether it was $5,000, $50,000, or more. We don't know. We do not know whether he received payments from Russian or other foreign sources or on separate occasions or whether he sought approval from the Pentagon or Congress to accept these payments. We don't know.

Related to today's hearing, we do not know what effect this potentially serious violation of the Constitution should or will have on General Flynn's security clearance.

Security clearance holders and those applying for security clearances are required to report their contacts with foreign officials. We do not know what, if anything, General Flynn reported about his contacts with officials from Russia or other countries. We do not know if he reported this one payment or any other payment he may have received. These are the questions that need to be answered.

We also have questions about the individuals who may seek to join the administration and obtain access to classified information while they are currently under investigation.

For example, there have been reports that President Trump's former campaign chairman, Paul Manafort, has been advising the White House recently while at the same time he's, reportedly, under FBI investigation for his dealings with Russian interests. We want to know how security clearances are handled if the existing clearance holders or new applicants are under criminal investigation. Does the FBI allow these individuals to continue to have access to classified information, or is there a process to place a hold on someone's clearance or application until the investigation resolves the questions?

Finally, President Trump claims that Democrats only became interested in Russian hacking for political reasons and that, for example, we have no interest in cyber attacks against OPM. He stated, and I quote, "They didn't make a big deal of that," end of quote.

The President is one million percent wrong. I and other Democrats worked aggressively on this committee's investigation of the attacks on OPM. We held multiple hearings, including one that I requested. We conducted extensive interviews and briefings with

key witnesses. We reviewed more than 10,000 pages of documents, and we issued two reports from the majority and minority staff.

I called for expanding our investigation to other agencies, including the State Department, the postal service, which were both attacked.

I called for investigating the cyber attacks on financial institutions like JPMorgan Chase. Our intelligence agencies had warned us—I called for investigating the cyber attacks on the Nation's biggest for-profit hospital chain, Community Health Systems, which had the largest hacking-related health information breach ever reported.

And I called for investigating the cyber attacks on retail companies, including Home Depot, Target, and Kmart. So the President's claim that we are focusing on Russia's hacking for political reasons is ludicrous. Our intelligence agencies have warned us that if we do not act now, our adversaries, including Russia, are determined to strike again. We need to get answers to these questions immediately, and I thank all of our witnesses for being with us today.

And, again, Mr. Chairman, I thank you for this hearing. And I yield back.

Chairman CHAFFETZ. I thank the gentleman.

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

I now would like to recognize the panel of witnesses. We're pleased to welcome Ms. Kathleen McGettigan, who is the acting director of the United States Office of Personnel Management.

Ms. McGettigan is accompanied by David DeVries—DeVries, sorry—chief information office of the United States Office of Personnel Management; Mr. Cord Chase, chief information security officer at the United States Office of Personnel Management, and Mr. Charles Phalen, director of the National Background Investigations Bureau, or NBIB. Their expertise on this issue will be very important to this subject matter, so they will all—everybody will be sworn in.

We're also honored to have Mr. Terry Halvorsen is the chief information officer at the United States Department of Defense. It's my understanding Mr. Halvorsen is retiring at the end of the month, and we could think of no better gift for you than having to testify before Congress.

It's such a joy. I know you're looking forward to it personally. So happy birthday, Merry Christmas, and happy retirement for coming to testify before Congress. But we thank you, sir for your——

Mr. HALVORSEN. Thank you.

Chairman CHAFFETZ. —for your service to this country and at the Department of Defense. And we really do appreciate your expertise and look forward to hearing your testimony. And we wish you well.

And, again, thank you for your service and your willingness to be here today. You probably could have squirmed out of this one if you really wanted to, but you stepped up to the plate and took this assignment, so thank you, sir, for being here.

Again, we welcome you all. Pursuant to committee rules, all witnesses are to be sworn before they testify. So if you would please rise and raise your right hand.

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

Thank you. You may be seated. Let the record reflect that the witnesses all answered in the affirmative.

Your entire written statement will be made part of the record, but we would appreciate it if you could keep your comments to 5 minutes. And like I said, your whole record—your whole testimony and any supplements you have will be made part of the record.

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

WITNESS STATEMENTS

STATEMENT OF KATHLEEN MCGETTIGAN

Ms. MCGETTIGAN. Good morning, Mr. Chairman, Ranking Member, and distinguished members of the committee. Thank you for the opportunity for my colleagues and myself to testify on behalf of the Office of Personnel Management.

As you said, I am joined today by Mr. Charles Phalen, the director of the National Background Investigations Bureau, Mr. Dave DeVries, OPM's chief information officer, and Mr. Cord Chase, OPM's chief information security officer.

While I am presently the acting director of OPM, I do have over 25 years of service at the agency.

OPM recognizes how critical the topics of today's hearing are to the Federal Government and to our national security, and I look forward to our having a productive conversation about the NBIB transition, the security clearance process, and information technology security.

As you know, the NBIB was established on October 1st, 2016, and is the primary provider of background investigations for the Federal Government.

Charlie has a distinguished career in multiple roles at senior levels in the Federal Government and private industry. His career has been focused on national security. His experience includes serving in capacities at the CIA, including as director of security and with the FBI as assistant director leading its security division.

NBIB is designed with an enhanced focus on national security, customer service, and continuous process improvement. Its new organizational structure is aimed at leveraging record automation, transforming business processes, and enhancing customer engagement and transparency.

In late 2014, OPM's market capacity for contract investigation services was drastically reduced by the loss of OPM's largest field contractor. This resulted in an investigative backlog. This backlog was exacerbated by the cybersecurity incidents at OPM that were announced in 2015.

Looking forward, it is an NBIB priority to address the investigative backlog while maintaining a commitment to quality.

To accomplish this, NBIB is focusing efforts in three primary areas: First, we are working to increase capacity by hiring new Federal investigators and increasing the number of investigative field work contracts.

Second, NBIB is focusing on policy and process changes to ensure efficient operations.

Third, NBIB has actively worked with customer agencies to prioritize the cases that are most critical to our national security.

Information technology also plays a central role in NBIB's ability to enhance the background investigation process. While still in development, NBIB's new system, NBIS, will be operated and maintained by DOD on behalf of NBIB.

On OPM's behalf, this effort is being led by our new chief information officer, David DeVries. Dave joined us in September of 2016. He is the DOD's principle deputy CIO, and he has a strong relationship with his former agency.

As we work to strengthen the infrastructure and security of NBIB, we are also working on fortifying our entire technology ecosystem.

As the Federal Government modernizes how it does business, OPM has focused on bracing new tools and technology to deliver optimum customer service and enhanced security.

OPM enhanced its cybersecurity efforts from multiple angles. We have added cybersecurity tools and security updates. We've implemented staff and agencywide training we've hired critical personnel and, finally, we continue to collaborate with our interagency partners.

Touching on efforts I've just outlined, our cybersecurity tools and security updates include 100 percent multifactor user authentication to access OPM's network. This is done via the use of PIV cards and major IT system compliance initiatives. Furthermore, OPM recognizes that cybersecurity is not just about technology, but it is also about people.

OPM has added seasoned cybersecurity and IT experts to its already talented team. OPM has hired a number of new senior IT managers and leaders and realigned and centralized its cybersecurity program and resources under the chief information security officer. In this capacity, Cord is responsible for taking the steps necessary to secure and control access to sensitive information. OPM also strengthened its threat awareness by enrolling in multiple information and intelligence sharing programs.

In conclusion, the necessary key partnerships and plans have been developed to build out NBIB and improve the security and efficiency of OPM's IT systems. These structural and process improvements will enable us to improve timeliness, reduce the background investigation. Equally productive is the CIO's holistic approach which ranges from bringing on qualified personnel to adopting new tools and procedures that enhance the security of OPM's networks and data.

Thank you for the invitation to testify before you today, and we welcome any questions you may have.

[Prepared statement of Ms. McGettigan follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF
KATHLEEN MCGETTIGAN
ACTING DIRECTOR
U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

on

Improving Security and Efficiency at OPM and the National Background Investigations Bureau

---

February 2, 2017

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

Good morning Mr. Chairman, Ranking Member, and distinguished Members of the Committee. Thank you for the opportunity for myself and my colleagues with me today to testify before the committee on the National Background Investigations Bureau (NBIB) transition, the security clearance process, and information technology (IT) security. As the Acting Director of the U.S. Office of Personnel Management (OPM), I can assure you we recognize how critical this is to the Federal government and to our national security. In keeping with our focus on modernizing the way that OPM carries out its important missions, OPM has worked to optimize the business processes surrounding background investigations. OPM has also taken aggressive measures to enhance the security of its IT systems, both within the NBIB and throughout OPM, accelerating an ambitious long-term IT security and modernization plan to upgrade the security of our systems and strengthen the agency's ability to respond to cyber incidents. OPM has also partnered with the Department of Defense (DOD) and other agencies to leverage government-wide knowledge, resources, and best practices.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

The National Background Investigations Bureau

NBIB was established on October 1, 2016, and is the primary provider of background investigations for the Federal government. NBIB is designed with an enhanced focus on national security, customer service, and continuous process improvement to meet this critical government-wide need. Charles S. Phalen, Jr., the NBIB Director, has a long and distinguished career in multiple roles at senior levels in the Federal government and private industry with a focus on protecting our national security. His extensive experience includes serving in various capacities at the Central Intelligence Agency, including as the Director of Security, and with the Federal Bureau of Investigations as Assistant Director leading its Security Division.

NBIB conducts 95 percent of investigations across the government. Even those few agencies that have the statutory authority to conduct their own investigations, such as the Intelligence Community, rely on NBIB's services in some capacity. Its new organizational structure is aimed at leveraging automation, transforming business processes, and enhancing customer engagement and transparency. Through a strong partnership with DOD, NBIB will build a modern and secure IT system to comprehensively support the investigations process and enhance end-to-end processes across government. These efforts will ultimately improve the efficiency, cost effectiveness, and quality of the investigations across the Federal government.

As you are likely aware, in late 2014, OPM's market capacity for contract investigation services was drastically reduced by the loss of OPM's largest field contractor, resulting in an investigative backlog. This backlog was exacerbated by the cybersecurity incidents at OPM that were announced in 2015. Looking forward, it is an NBIB priority to address the investigative backlog while maintaining a commitment to quality and returning back to the level of performance realized from 2009 through 2014. NBIB, working with the Office of the Director of National Intelligence (ODNI), DOD and other customers, is focusing efforts in three primary areas. First and foremost, NBIB is working to increase capacity. NBIB hired 400 new Federal investigators in 2016, and NBIB recently awarded a new investigative fieldwork contract, increasing the fieldwork contractors from two companies to four. Work under the new contracts began on February 1, 2017. Second, NBIB is focusing on policy and process changes to add efficiencies, reduce level of effort, and maintain investigative quality. To support this effort, NBIB, working closely with the DOD and interagency partners, conducted a detailed business process reengineering effort and worked in collaboration with ODNI in its role as the Security Executive Agent to identify appropriate policy and process changes to help address the backlog. Third, NBIB has actively worked with customer agencies to prioritize cases and schedule those that are most critical to our national security and the mission needs of our customers.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

Information technology also plays a central role in NBIB's ability to enhance the background investigation process. A key component of NBIB is to leverage DOD's cybersecurity expertise and resources to design, develop, and implement a modern and secure IT environment. While still in development, the new system, known as the National Background Investigation System (NBIS), is to be operated and maintained by DOD on behalf of NBIB. NBIB is encouraged by the significant progress DOD has made toward new capabilities that will improve the effectiveness and security of background investigations. Concurrently, the OPM Office of the Chief Information Officer (OPM CIO), in coordination with our interagency partners to include DOD and Department of Homeland Security (DHS), has aggressively pursued further improving the cybersecurity posture of the OPM network.

Role of the Office of the Chief Information Officer

OPM has worked to strengthen the infrastructure and security of not only NBIB, but also OPM's entire technology ecosystem. This effort is being led by OPM's new CIO, David DeVries, who joined OPM in September 2016. Mr. DeVries had previously been the DOD Principal Deputy CIO and has a strong relationship with his former agency that facilitates coordinating the implementation of NBIS. Indeed, as the Federal government modernizes how it does business, OPM has focused on embracing new tools and technologies to deliver optimum customer service and enhance the security of the information we house. In a rapidly changing and increasingly interconnected digital world, it is important for agencies to develop the best possible defenses and safeguards.

Over the past eight months, OPM has successfully begun to roll out its program for implementation of the Federal Information Technology Acquisition Reform Act and enhanced the agency's infrastructure in ways that will help OPM support its cybersecurity initiatives and strategies, ensure its IT programs run more efficiently and securely in supporting the OPM business lines, and better utilize limited resources.

OPM has enhanced its cybersecurity efforts from multiple angles: through the addition of cybersecurity tools and security updates; through staff and agency-wide training; through hiring critical personnel; and through collaboration with OPM's interagency partners. For example, in Fiscal Year 2016, OPM implemented 100 percent multi-factor user authentication for access to OPM's network, via the use of the "Personal Identity Verification" (PIV) card. This capability and enforcement provides a powerful barrier to our networks and information stores from individuals who are not authorized to have access. OPM is in the process of expanding this to agency applications to further increase the security of our systems. In 2016, OPM launched two major IT system compliance initiatives that resulted in all major IT systems having current ATO (Authority to Operate) and network segmentation.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

As the Federal government's personnel agency, OPM recognizes that cybersecurity is not just about technology, but is also about people and, to that end, in addition to strengthening its technology, OPM has added seasoned cybersecurity and IT experts to its already talented team. OPM has hired a number of other new senior IT leaders, and realigned and centralized its cybersecurity program and resources under the Chief Information Security Officer (CISO), a primary responsibility of which is to take the steps necessary to secure and control access to sensitive information. OPM also hired Information System Security Officers (ISSOs) in Fiscal Year 2016 to support all of OPM's major information systems.

OPM is continuing to leverage and utilize its interagency partnerships and the expertise of the IT and cyber communities across government. OPM strengthened its threat awareness by enrolling in multiple information and intelligence sharing programs. OPM was one of the first agencies to participate in DHS's Einstein 3A program, and was one of the first agencies in the Federal government to fully implement Phase 1 of DHS's Continuous Diagnostics and Mitigation program. These initiatives allow agencies to detect and prevent cyber-attacks, and continuously identify and proactively mitigate cybersecurity threats and vulnerabilities that might arise.

The cybersecurity incidents at OPM provided an important catalyst for accelerated change across the Federal government. OPM met the challenge and greatly appreciates the collaborative spirit with which its interagency partners across government continue to work with us every day. Embracing modernization can help save taxpayer dollars, improve critical programs, and mitigate security risks in a world of continually evolving threats. OPM and DOD will continue to collaborate on the development of a state-of-the-art IT system for NBIB. By investing in IT systems across functions, we can drive more effective, efficient, and data-driven accomplishment of work across a variety of missions.

Conclusion

The necessary key partnerships and plans have been developed to build out the NBIB and improve the security and efficiency of OPM's IT systems. We created a coordinated strategy to transition the investigative program to an organizational model that fosters innovation, focuses on customer service, and leverages interagency expertise. These structural and process improvements, in coordination with our partners, will enable us to improve timeliness and reduce the investigative backlog. In parallel, we are working closely with DOD's CIO to build the information systems capabilities to support this activity for now and the future. This productive partnership will enable an effective and secure information environment as a government-wide solution. Equally productive is the CIO's holistic approach, which ranges from bringing on new qualified personnel to adopting new tools and procedures that enhance the security of OPM's networks and data for all of OPM's lines of business, including NBIB.

Statement of Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management

February 2, 2017

Thank you for the opportunity to testify before you today, and we welcome any questions you may have.

Chairman CHAFFETZ. Thank you. Thank you for your testimony.

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

My understanding is maybe yourself, Mr. Chase, and Mr. Phalen, I don't know if you have opening statements or if you care to say anything, but I'll recognize each of you. If you don't have anything, we'll just—Mr. DeVries, do you have——

STATEMENT OF DAVID DEVRIES

Mr. DEVRIES. Thank you, Mr. Chairman.

I'd like to just take this opportunity to thank you for the opportunity to come here. As the brief bio was read there, I did come from 30 years in the Army. I transitioned in in 2009 to become a senior executive within DOD, and where I spent the last 2–1/2 years as the principle deputy for the DOD CIO.

Broad range here, I was asked to come here to OPM and accepted that and arrived here in September of 2016. And it's a pleasure being here today, and I enjoy the opportunity to answer your questions here. Thank you.

Chairman CHAFFETZ. Thank you.

Mr. Chase.

STATEMENT OF CORD CHASE

Mr. CHASE. Thank you very much for the opportunity——

Chairman CHAFFETZ. If you can all bring that—I'm sorry. You've got to bring the microphones up close, uncomfortably close to make sure we can all hear you.

Mr. CHASE. Again, thank you very much for the opportunity to speak today. One of the things that I want to make clear is I ran into the fire to help with the events that occurred in 2015. In the rebuilding process, we've made a lot of advancements, but it's only to get us to a standard environment. By no means am I up here saying, we're successful or we've won anything, that we're doing our best to improve the environment to secure the information within OPM and NBIB.

With that, there are quite a few items that I'd be happy to discuss with all of you on those improvements, and that's all I have at this point.

Chairman CHAFFETZ. Thank you.

Mr. Phalen.

STATEMENT OF CHARLES PHALEN

Mr. PHALEN. Thank you, Mr. Chairman. I'm happy to be here and join with you today in a good conversation on this.

To echo a little bit what Ms. McGettigan mentioned, we are focused in our—as we begin our—or end our 4th month as an entity on three key things.

One is recovering and increasing our capacity to do background investigations, improving our capability to gather information that is relevant to background investigations and, finally, working on those innovations that will help us in partnership with the security executive agent and the suitability executive agent to look at what an investigation will look like as we move down into the future.

A key to this is building an organizational structure beyond what existed on September 29th and adding capabilities in terms of investments and in terms of innovation, and then very importantly, working in partnership with DOD as we build out an information technology systems that will be able to enhance and inform security investigations across our entire spectrum of about 100 customers across the Federal Government.

With that, I'm very happy to be here. Thank you for the opportunity today.

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 the opportunity to testify before the committee today on the Department's information technology and cybersecurity support to the National Background Investigations Bureau.

I am Terry Halvorsen, the Department of Defense chief information officer. You have my opening statement. I think most of you are familiar with my responsibilities, so in the interest of time, I'll cut this a little short.

The department is responsible for the development and securing the NBIB IT systems. We have brought the full expertise of the department both in IT and cybersecurity resources to bear on this problem, and it is our objective to replace the current background investigations information system with a more reliable, flexible, and secure system in support of the NBIB.

Defense information system under the DOD's CIO's oversight has established the National Background Investigations Systems Program Management Office to implement this effort. The PMO is responsible for the design, develop, and operation of the IT systems capabilities needed to support the investigative process to include ensuring that the cybersecurity protections and resiliency of these capabilities. The alignment of the systems under DOD assures we leverage all national security systems expertise and capability to protect the background investigation data. And I assure you, we are doing that.

The Department has made significant headway on this important mission, since I previously testified before this committee last February, and we are on track to deliver the capabilities needed in an iterative fashion using DOD expertise and best industry practices.

In fiscal year 2016, the Department funded preacquisition activities to better posture for official standup and funding in fiscal year 2017. I would like to thank Congress and members of this committee for supporting the Department's funding request for NBIB IT infrastructure and cybersecurity modernization. As you know, the fiscal year 2000 continuing resolution did include new start authority for the NBIB, and we thank you for that.

Today, several of the NBIB's prototypes are enabling the Department to work with industry and other partners to discover capabilities that we will provide with a more efficient, effective, and secure background investigation system in the future.

Throughout this process, we are actively partnering with industry, integrating commercial feedback into the process to ensure we are focusing on capabilities and keeping up with the changing pace of technology.

I am pleased with the current progress on NBIS that the Department and our partners have made to date. I look forward to seeing what this organization will accomplish as it makes progress toward delivering several prototype capabilities by the end of fiscal year 2017 and an initial operating capability covering the full investigative process in the fourth quarter of 2018.

This is an important opportunity for the Federal Government to strengthen the security of the IT infrastructure that supports the Federal background investigating process. This approach utilizes the Department's recognized IT cybersecurity expertise, best industry practices while maintaining a streamline centralized governmentwide approach to the investigative services that the NBIB provides today for more than 100 different Federal agencies.

Thank you for this committee's continued support, and I look forward to 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

THE NATIONAL BACKGROUND INVESTIGATIONS BUREAU

TRANSITON, RELATED INFORMATION TECHNOLOGY SECURITY,

AND THE SECURITY CLEARANCE

INVESTIGATION PROCESS

FEBRUARY 2, 2017

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 (IT) and cybersecurity support to the National Background Investigations Bureau (NBIB). 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, the DoD CIO is responsible for all matters relating to the DoD information enterprise, including cybersecurity for the Department. In this capacity, the DoD CIO is responsible for oversight of the Department's efforts to design, build, operate, secure, and defend a new IT system to support the background investigative processes for the NBIB. NBIB provides investigative services for more than 100 Federal agencies to make decisions to determine whether individuals meet requirements for new or continued employment; are eligible to hold a sensitive position; or are eligible for access to Federal facilities, automated systems, or classified information. The relationship between DoD and OPM is strong and has been critical to our success thus far on NBIB. David De Vries, OPM's Chief Information Officer, who was previously serving as the Principal Deputy DoD CIO, has helped strengthen that relationship and brings critical IT and cybersecurity expertise to OPM.

As the Department's focal point for the new background investigations IT system, the DoD CIO brings together the Department's full range of IT and cybersecurity resources and expertise. DoD's objective is to replace the current background investigations information systems with a more reliable, flexible, and secure system in support of the NBIB. The Defense Information Systems Agency (DISA), under the DoD CIO's oversight, has established the National Background Investigation System (NBIS) Program Management Office (PMO) to implement this effort. The NBIS PMO is responsible for the design, development, and operation of the IT system capabilities needed to support the NBIB investigative process – to include ensuring cybersecurity protections and resiliency of these capabilities. The alignment of NBIB systems under DoD assures we leverage all national security systems expertise and capability to protect background investigation data.

The Department has made significant headway on this important mission since I previously testified before this Committee last February, and are on track to deliver the capabilities needed in an iterative fashion.

In fiscal year 2016, the Department funded pre-acquisition activities to better posture for official standup and funding in fiscal year 2017. I would like to thank Congress for supporting the Department's funding request for NBIB IT infrastructure and cybersecurity modernization efforts. The fiscal year 2017 continuing resolution (CR) included new start authority for NBIS, which has allowed us to make progress, including awarding a contract last month for the case management prototype. Today, several NBIS prototypes are enabling the Department to work

with industry and discover capabilities that will provide NBIB with a more efficient, effective, secure background investigation IT system in the future. Throughout this process, we are actively partnering with industry and integrating commercial feedback into the process, to ensure that we are focusing on capabilities and keeping up with the changing pace of technology.

Conclusion

I am pleased with the current progress on NBIS that the Department has made to date, and I look forward to seeing what this organization will accomplish as it makes progress toward delivering several prototype capabilities by the end of fiscal year 2017 and initial operating capability covering the full investigative process in the fourth quarter of 2018. This is an important opportunity for the Federal Government to strengthen the security of the IT infrastructure that supports the federal background investigations process. This approach utilizes the Department's recognized IT and cybersecurity expertise, while maintaining a streamlined, centralized, Government-wide approach to the investigations services that NBIB provides today for more than 100 different Federal agencies. I want to thank you for this Committee's continued support for NBIB, and I look forward to your questions.

Chairman CHAFFETZ. Thank you.

I will now like to recognize the gentleman from Texas, the chairman of the subcommittee on Information Technology, Mr. Hurd.

Mr. HURD. Thank you, Mr. Chairman. I want to thank you and the ranking member for the continued diligence on this important issue.

Mr. Phalen, I've got some basic questions for you. Sorry for the basicness of the questions.

You're in charge, right?

Mr. PHALEN. Yes, sir.

Mr. HURD. Do you have a technical background?

Mr. PHALEN. I do not have a technical background.

Mr. HURD. Who is the person directly reporting to you that is responsible for preventing another attack that we saw, like the one we saw a number of months ago?

Mr. PHALEN. So it is not a direct chain——

Chairman CHAFFETZ. Sorry. Mr. Phalen, if you could move that microphone. Straighten it up and right—right up next—there you go. Thank you.

Mr. PHALEN. There you go. Okay thank you.

There's no one specifically in my chain of command that is immediately responsible. We rely on Mr. DeVries and Mr. Chase as the CIO and CISO to provide the security for the systems that we are operating today.

Mr. HURD. Copy.

So Mr. Chase, you are in charge.

Mr. CHASE. That is correct, for cybersecurity.

Mr. HURD. Well, thank you for running into the fire.

Mr. CHASE. Thank you.

Mr. HURD. I recognize the difficulty of the task. In your brief remarks, you talked about the first step was getting OPM up to a baseline.

Mr. CHASE. Correct.

Mr. HURD. Can you take 90 seconds and explain that baseline?

Mr. CHASE. Sure. That's a good question. So one of the things, when I came on board, was to set an appropriate strategy and a pathway forward. So it was the stabilization phase. So we understood that there were quite a few systems that were out of compliance. So we knew that we had to take steps to get those back into compliance.

We also had another layer of engineering tasks, which included network segmentation, making sure that we had the appropriate monitoring tools in place, and then the tuning process to support that.

Throughout fiscal year 2016, we were able to get those accomplished but, again, to a standard baseline where we feel comfortable that we can control our environment and we understand where we were with the IT system boundaries and the IT system boundary inventories.

Mr. HURD. So of the IG GAO, they've all done reviews, there's been a number of outstanding issues. Many of the outstanding issues for years had been on the IG report and the GAO high-risk report.

Of those documents, how many of those vulnerabilities, that have been identified, are still outstanding?

Mr. CHASE. So there are still items that are outstanding, and we prioritized them based on their criticality——

Mr. HURD. What's the highest priority—highest priority vulnerability that's still outstanding?

Mr. CHASE. So the IT system compliance was the most significant vulnerability that was identified in the Fiscal Year 2016 FISMA report, as well as the IT security officer hiring process, which is something we were able to accomplish at the end of this year as well.

Mr. HURD. Good copy.

You talked about segmentation. And we saw after the breaches in 2014 and 2015, the hackers were able to basically move, you know, without—with impunity through the network. And my question is what have you done to make life harder on the hackers that once they get past your defenses?

And I will say my—you know, I begin with the presumption of breach, you give an attacker enough time, they have enough resources, they are going to get in, so what do you do once they get in, and how have you improved segmentation across the OPM network.

Mr. CHASE. So I consider it a level of effort, so I'm trying to make it as hard as possible for them to get in. Understanding that OPM is a customer-oriented agency and has to communicate. Some of the segmentation that we have done is identify all of our major systems and high-valued assets within our environment, as well as, all the privileged and nonprivileged users.

We segmented those between each other and set the appropriate firewalls and monitoring tools to ensure that one can't get to the another and vice versa, and if there are attempts to get between the other, the other is stopped and flagged, and there's a follow-up with that event itself.

Mr. HURD. In my remaining minutes, I want to ask a question. And I don't mean to be indelicate. Why did we get to this situation? And I ask that question in order to learn from this experience so we can take those lessons learned and apply it across the Federal Government.

Mr. CHASE. So I'm going to say I came post breach, and I know there's quite a few lessons learned. There was a majority and minority reports issued, there's all the audits that were issued, and that's what I've been going off of and, again, trying to apply those to prioritize the next steps to be able suppress the threat and the risks within OPM.

Mr. HURD. So why—you've been there now for enough time. You've seen the problems. You've probably been shocked by some of the deficiencies within the network. Why do you think that network got to where it was?

Mr. CHASE. I would say based on those reports and information that was put in front of me, there were systematic failures within OPM that led to it.

Mr. HURD. Mr. Chairman, I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the ranking member of the subcommittee on IT, Ms. Kelly from Illinois, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair.

And thank you all for your testimony here today. This is actually the committee's third hearing on the OPM data breach.

The data breach compromised the information of millions of Federal employees. The committee responded almost immediately and did an extensive bipartisan investigation into the incident. In total, committee staff reviewed more than 10,000 pages of documents, interviewed multiple witnesses, and had numerous briefings from both Federal and nonFederal entities. I applaud the work we have done on the OPM data breach, but I must address the elephant in the room.

We are holding a hearing about hacking by a sophisticated actor, likely a State actor for a hack that occurred more than a year ago. But this committee has chosen not to take any action to investigate the recent Russian hacking and propaganda campaign to impact our election.

Only last month, the NSA, FBI, and CIA concluded with a high degree of confidence that Russia successfully hacked groups throughout our Nation in an effort to influence our election. In the face of this report from our top intelligence agencies, we have done zero oversight into this issue. There's not been a single hearing or request.

My wonderful chairman on the IT subcommittee asked Mr. Chase about lessons learned.

Mr. Halvorsen, I would like to ask you about lessons learned after the vulnerabilities were exposed in the OPM data breach.

Mr. HALVORSEN. We certainly took the vulnerabilities that were exposed in the database, and I can assure you that both in the OPM legacy systems, the work they're doing today and in the new systems, we are taking those lessened learn and making sure that the systems we are building new are built from the ground up with cybersecurity baked in, and that we've assumed from the beginning that this system could be penetrated.

So there's a condition we have that you might hear in the Navy termed, it's set conditions ZEBRA, it means close the watertight doors. We are making sure that the new system will be segmented enough that we can close the doors. Because there's two things you want to stop. Certainly, you want to stop people from getting in, but when they get in, you don't want your answer to be you've got to shut the system down. That's a victory.

So we're designing this system so that we can fight—and that is the correct word—fight through any attempt to breach this system. And if we get breached, be able to block and contain and then eradicate any malware system loss that gets in here.

Ms. KELLY. Thank you.

Did the subsequent investigations help in understanding how things could be improved?

Mr. HALVORSEN. Absolutely.

Ms. KELLY. Anybody else want to answer that?

Mr. HALVORSEN. Yes, they did.

Ms. KELLY. And any of the other witnesses?

Mr. CHASE. I concur.

Mr. DEVRIES. Concur.

Ms. KELLY. Thank you.

I believe these OPM investigations went a long way in assuring the American public that everything possible was being looked at to prevent this from happening again. But it is clear that politics have prevented this committee from being willing or able to do the necessary objective and nonpartisan oversight on the Russian attack. That's why I, and every one of my democratic colleagues in the House, have signed on to legislation to establish an independent bipartisan commission to investigate foreign interference in the 2016 elections. Thank you for your response.

And, Chairman, I yield back.

Chairman CHAFFETZ. Will the gentleman—gentlewoman yield first?

Ms. KELLY. Of course.

Chairman CHAFFETZ. As I've said publicly, and the gentlewoman should know, given that it involves sources and methods, the United States Congress is organized such that the House Intelligence Committee takes the lead on those things. We can investigate anything at any time, but I do have limits in that I cannot investigate sources and methods which clearly is the purview of the House Intelligence Committee.

I would also suggest that we were the first committee to create a subcommittee specifically on information technology. We were the first to dive into the OPM data breach, and we have been pushing from the Department of Education and others to make sure that we do have the proper defenses in place. And to suggest that it's only one particular country would be naive at best. And it could be everything from a guy in a van down by the river down to a Nation State.

Ms. KELLY. We know it was the Russians in this particular instance.

Chairman CHAFFETZ. And I think that should be investigated. I have said as much publicly, and I've also—I think everybody should know, every Member of Congress should know that the House Intelligence Committee is really the only organization within Congress that is set up to be able to do that.

Mr. CUMMINGS. Would the gentlelady yield, please?

Ms. KELLY. Yes, I will.

Mr. CUMMINGS. Very briefly, Congressman Swalwell and I, over a month ago—as a matter of fact, in December, filed a bill which asks that we have a 9/11-type investigation. And the reason why we did that is because we didn't want it to get mired in a political battle like the Benghazi Committee did, Select Committee.

And it would be patterned after the 9/11 commission so that we would bring America's best experts to the table. It would be an equal number of Democrats, an equal number of Republicans, and that they would look at this thing carefully—and with the chair's indulgence, I need to explain this—and they would come back with recommendations. They would have subpoena power.

Then we refiled that bill in January when the new session came in. Every single Democrat in the Congress signed on to that bill. Not one signal Republican signed on. And one of the reasons why we did that is because we felt we didn't move to common ground;

we need to move to higher ground, that this was such a serious attack on our democracy, and our election process, that it deserved that kind of attention. And so that bill is still out there. Only Democrats have signed on.

One of the things we were concerned about is the chairman of the Intelligence Committee, Mr. Nunes, was a part of the transition team for President Trump. And we just felt that we needed to take the complete thing out and let an independent body do it. And I just wanted to explain that to the gentlelady.

Thank you very much. And thank you for yielding. Nice job, by the way.

Chairman CHAFFETZ. I'll now recognize the gentleman from Florida, Mr. DeSantis, for 5 minutes.

Mr. DESANTIS. Thank you, Mr. Chairman.

Ms. McGettigan, I know after the OPM breach there's several months people were, kind of, notified. But I've had people, constituents, just wonder, I mean, what has been done to mitigate the potential damage to people whose files were compromised?

Ms. MCGETTIGAN. Thank you for that question.

We have entered into—in December, we entered into a contract and identity protection contract. We expanded the coverage that we already had. And we are moving toward having coverage for 10 years. The current contract covers all those affected by the two breaches, and it runs out in December of 2018 during——

Mr. DESANTIS. What would that mean, just for somebody who had their stuff compromised?

Ms. MCGETTIGAN. I'm sorry. We have identity protection services and credit monitoring. So people have received—people who were affected have received information on how to sign up for the credit monitoring, although they are covered by insurance whether they sign up or not.

And currently, the ceiling on the insurance we have expanded to $5 million, and we are moving toward complying with congressional direction to have the contract go for 10 years of credit monitoring.

Mr. DESANTIS. Okay. Good. I mean, I think that we in this committee—and I applaud the chairman for being on this issue. And we hear about these other hacks and stuff. This was catastrophic. I mean, you're talking about these files with the amount of information that's there, and I had to go through it in the military, and other people, perhaps, you guys have gone through it, too, there is a lot, a lot of information there, and it's a massive vulnerability. So I hope that what's being done is going to be effective.

Let me ask—this may be Mr. Chase or maybe someone else want to take this. If OPM suffers another compromise and NBIB applications and its systems are breached, who makes the final call as to whether or not the compromised applications are taken offline or continue to run?

Mr. HALVORSEN. If it's in the new systems that are developed, that is me.

Mr. DESANTIS. Do you agree with that?

Mr. DEVRIES. For the new system, yes. Right now we're currently operating underneath the existing legacy system.

Mr. DESANTIS. What's the answer——

Mr. DEVRIES. The answer is the CIO gets the report of it from the CISO, and the director makes the call on it.

Mr. DESANTIS. Okay. Let me ask you this, because the majority staff on this committee had a report indicating that there were certain tools following some of the previous breaches that were bought, and then they there were delayed in terms of their deployment for a variety of reasons, but one of them, that they had to make certain notification to relevant unions.

So what kind of notifications is the IT security team required to make before deploying these tools, and what is the purpose of the notifications?

Mr. CHASE. So from post breach coming in, any tool that we go out on the street to market and do our research on is fully vetted internally. We have a procurement office inside of OPM that works with us to make sure that the appropriate language is put into that, and then we move to the process of deploying that tool.

Mr. DESANTIS. But in terms of the delays, have there been delays because of notification requirements?

Mr. CHASE. I'm not aware of that specific statement.

Mr. DESANTIS. Okay. Had there been other barriers or challenges in trying to timely deploy some of these tools, bureaucratic roadblocks?

Mr. CHASE. Again, post breach, based on the situation—and, again, I mentioned earlier stabilizing, the procurement office has been very, very flexible with me and making sure that they can give us the time——

Mr. DESANTIS. But this was so—the implication is there may have been a problem prebreach?

Mr. CHASE. I'm not aware outside of what I'm reading in those reports.

Mr. DESANTIS. Do you think that it was a problem?

Mr. DEVRIES. I have no firsthand knowledge of that, but just from the acquisition side and having been in this field for many years, yes.

Mr. DESANTIS. Okay.

Well, I will yield back the balance of my time.

Chairman CHAFFETZ. I thank the gentleman.

I now recognize the gentleman from Massachusetts, Mr. Lynch for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

And I want to thank our witnesses for your great work and for your willingness to help us. I want to revisit the issue raised by Ms. Kelly about the unwillingness or the inability of the committee to really investigate what's going on with the Russian hacking.

But before I get into that, let's talk a little bit about the issue that brings you here.

In June and July of 2015, OPM publicly disclosed that its information technology systems had been experiencing massive data breaches over some time, compromising the Social Security numbers, birthdates, home addresses, background investigation records, and other highly sensitive personal information belonging to about 22 million individuals.

These cyber breaches were not only devastating in terms of their impact on the financial security of their victims, rather, they also

posed a grave national security threat as the extensive security clearance questionnaires, about an 80-page document, that really drills down on folks and was filled—were filled out by nearly 20 million Americans who have security clearance rights and privileges, and the names and the information of those individuals were included among the data.

I had asked—that was a—that was a terrible—you know, some people call that a—like a cyber Pearl Harbor, because all our folks who are actually actively interested in working on our national security organizations, you know, basically, they were giving up. And so I asked at a very basic level, I asked, Ms. Archuleta, who was running the OPM at the time, I said, have you actually gone back and encrypted the Social Security numbers of these employees? Were they encrypted? And she said, no, they were not. So—so all those Social Security numbers of those 22 million people went out.

And then a year later, we had one of her successors—not her successor, but one of the people under her, I asked, again, have we encrypted the Social Security numbers of the people, the 22 million people? And they said there are still—there are still vulnerabilities we still haven't been able to do that.

So let me ask, have we encrypted at least the Social Security numbers of these 22 million people?

Mr. DEVRIES. Sir, I'll take that for the record. Yes, we have begun a vigorous program in 2016 to encrypt the databases. So it's not just encrypting the Social Security number, but it is the databases that contain those critical information.

Mr. LYNCH. Are we done with that yet?

Mr. DEVRIES. We are not completely done across the whole OPM environment, but the HVA systems we have gone through, and I have one remaining system to be done, and that is scheduled for next month. To complete the——

Mr. LYNCH. What percentage of the 22 million have been encrypted? Can you give me an estimate on that?

Mr. DEVRIES. Of the NBIB system, which contains those records there, all but one have been encrypted.

Mr. LYNCH. So what's lacking in percentage?

Mr. DEVRIES. One major database there on the mainframe.

Mr. LYNCH. All right. You're not answering my question, but—look, we need to get that done. Okay?

Let me go on to the Russian thing. Look, we've got—I understand that the chairman's resistance on sources and methods, I get that. But we have—and I would like to introduce these into the record.

First of all, I would like to introduce into the record my letter from December 15th—14th asking for a hearing on the Russian hacking.

Secondly, I'd like to enter into the record an FBI investigation regarding Russian malicious cyber activity. They did a whole investigation on this. It's called "grisly steppe," s-t-e-p-p-e. I want to enter into the record a background to assessing Russian activities and intention into recent U.S. elections, the analytical process and cyber incident attribution. That's produced by the offices of the director of National Intelligence.

I would like to submit for the record, a statement for the record, worldwide threat assessment by James R. Clapper, director of the National Intelligence, February 9, 2016.

I ask for unanimous consent.

Chairman CHAFFETZ. Without objection, so ordered.

Mr. LYNCH. Thank you. So we have enough here. Just with this here, we have enough here to do an investigation. And this is just the stuff that is unclassified that the intelligence community has put out there. We don't have to talk about——

Chairman CHAFFETZ. Will the gentleman yield?

Mr. LYNCH. Yes. Sure I'll yield.

Chairman CHAFFETZ. Two points. Number one, sources and methods are the sole jurisdiction of the intelligence community.

Number two, have you really thought this through? Do you really think it's appropriate for this committee to investigate the specific hack of the DCCC?

Mr. LYNCH. Absolutely.

Chairman CHAFFETZ. Because if you are going to do an investigation of the DCCC, we're going to have to dive into a political party's infrastructure operation's data. I don't think that's appropriate. If you——

Mr. LYNCH. Let me—well——

Chairman CHAFFETZ. Here's the difference. Here's the difference——

Mr. LYNCH. Reclaiming my time. Actually, you know, you're using all my time here.

Look, look they hacked—they hacked the American election. That is worth looking into——

Chairman CHAFFETZ. There's no evidence of that. And President Obama said that that wasn't even possible.

Mr. LYNCH. This is high confidence. This is our own FBI, high confidence that they hacked the election, that they interfered with the election. It may not have been outcome determinative. I'm not saying that. But based on the FBI, based on the office of—the director of national security, they're saying, yeah. And also, the CIA, they're in agreement that the elections were hacked.

Now, I'm not saying they affected the outcome, but they tried. It may have been just chaos that they wanted to create, but they interfered with our elections. And if we're turning a blind eye to that, that's a shame. That's a shame. That's core to our democracy.

And look, if we're just going to say, oh, that's somebody's work, that's not anybody else's work. That's our work. There are plenty of reports here we can talk about, and we ought to do it publicly, about the damage done to the confidence in our electoral system. That's what's important here.

People have to—people have to fear that we have an integrity—a certain integrity in our own systems and that other countries are not allowed to interfere with that. That's a red line. We should not allow that. And it should be a very serious obligation of this committee to make sure that doesn't happen again.

And we need all the committees of jurisdiction to work on this. We're a committee of unlimited jurisdiction. The gentleman has said that quite frequently. That's the strength of this committee.

And I think this is—look, they hacked our election. This should be bipartisan. This should not be Democrat versus Republican.

Chairman CHAFFETZ. The gentleman's time—the gentleman's time is well expired.

As I said, I do think there should be—as I said when it happened, there should be an investigation. There should be a prosecution. They should go out——

Mr. LYNCH. These are the investigation of the committee.

Chairman CHAFFETZ. Hold on. The gentleman's time has expired.

The Intelligence Committee is the only one that can look at sources and methods. That is the rule of the House.

Mr. LYNCH. We won't look at sources and methods. We'll just look at what the agencies themselves have made public.

Chairman CHAFFETZ. The gentleman's time has expired.

And if you are going to do a proper investigation, as this committee did, with the breach at the Office of Personnel Management, you have to look at the two sides of the breach, those that were trying to do it, which this committee could not look at in the OPM breach. Again, that is the purview of the House Intelligence Committee.

But we could look at those that were breached and how inept their systems were and how bad it was set up and how the inspector general was warning of these things. That, we did do.

Mr. LYNCH. We had nine separate investigations of Hillary Clinton, nine separate investigations——

Chairman CHAFFETZ. The gentleman's—the gentleman is out of the order. The gentleman's time is expired. I gave you well more than 5 minutes.

What I think is inappropriate. And I'm trying to answer the question. It would be wholly inappropriate for the United States Congress, for us to dive into the DCCC. You might want to do an investigation yourself of the DCCC. I don't think that the United States Congress should be diving into their individual private systems of a political party. I think that's too broad—if you want me to start issuing subpoenas of the DCCC, I'm probably not going to do it, but go ahead and suggest it.

Mr. LYNCH. How about some of the FBI——

Chairman CHAFFETZ. The gentleman's time has expired.

Mr. LYNCH. You asked me a question.

Chairman CHAFFETZ. No, I did not. I did not.

Mr. LYNCH. And I'm trying to respond. You asked me if I wanted——

Chairman CHAFFETZ. I did not ask—the gentleman is out of order.

Mr. CUMMINGS. Would the chairman yield? Would the chairman yield? I think we need to calm down here a little bit.

Mr. Chairman, you have made some statements, and I just ask you to give him the courtesy of a minute and a half just to respond.

Chairman CHAFFETZ. No, I will not. I will not.

Mr. CUMMINGS. Well, would the gentleman let me finish? Thank you.

This has been an attack on our democracy, Mr. Chairman. And Mr. Lynch is one of our greatest members, and the passion that he has expressed is not limited to him, it's to many Americans. They

feel as if all of our—the things that underpin our democracy have been attacked over and over again.

And as I said yesterday, we keep saying we're going to wait till certain things happen with President Trump. They are happening now.

Chairman CHAFFETZ. Can I ask that——

Mr. CUMMINGS. And if the gentleman would just give me 30 more seconds.

And all I was saying is I was hoping that in—I mean, as a courtesy to the gentleman, I just wanted him to be able to respond.

Chairman CHAFFETZ. I'd like to ask you a question, if you don't mind, to my ranking member. Does the ranking member believe that this committee should do an investigation of the DCCC?

Mr. CUMMINGS. I think that we can look at certain things. I know I am very familiar with sources and methods, but I think what the gentleman is saying is let's just look at the things that are—that are unclassified. And apparently, he has his reports in his hand, and we can see where we go from there.

Number two, as I said before, in answering the chairman's question, we have a bill that would—I think, would resolve this issue very nicely.

I think the thing that I'm most concerned about, and I'm sure Mr. Lynch is concerned about is that we cannot just turn a blind eye to when we have 17 intelligence agencies who unanimously agree that there has been hacking with regard to our elections.

And there seems to be—one of the things that I've noticed, this has been an effort, not by you, Mr. Chairman, but by others to say, okay. It didn't affect the results. We don't even have to get there. Forget it. I accept President Trump as my President. I'm looking forward to meeting with him next week. But, the idea that Russia could come in and interfere with our elections, all of us should be going berserk. I mean, we should be—I mean, just really, really upset. And so all I'm saying to you is that I think all the gentleman is saying, is he's got documents that you've already entered into the record that are unclassified, want to look at those. Now, how far we can go is another thing.

But, again, Mr. Chairman, you and I know what happened with the Benghazi Committee. Basically, it became a partisan fight.

Chairman CHAFFETZ. I'll—hold on. The gentleman's time is expired here. You're going well—you're going well outside the scope of this——

Mr. CUMMINGS. No, I'm not.

Chairman CHAFFETZ. Yes. Yes.

Mr. CUMMINGS. I'm not and I would pray that you not do an Issa on me.

Chairman CHAFFETZ. I've given you ample time. I've given you more time——

Mr. CUMMINGS. Don't do an Issa on me, please. Don't do that.

Chairman CHAFFETZ. No. I'm asking you a simple question. I just want an answer to a simple question. If you don't want to answer it, it's fine.

Mr. CUMMINGS. I've answered it. I've told you.

Chairman CHAFFETZ. I'm going to ask one more time.

Mr. CUMMINGS. Yes. I've answered you. Okay? Yes. I just answered you.

Chairman CHAFFETZ. I just wanted——

Mr. CUMMINGS. I just answered you.

Chairman CHAFFETZ. Okay. I'm just saying——

Mr. CUMMINGS. You're not listening. What I said was what the gentleman asked. All he asked—he said, take the unclassified information. Do not turn a blind eye to an attack on our electoral system. Let's look—let's go as far as we can. When you take it to the Intelligence Committee, what you've done is you've gotten Mr. Nunes, who is on the transition—who is on the transition committee for President Trump.

And as much as I like him, I want—as the gentleman asks, he wants an investigation that will have integrity. And I—I appreciate integrity over and over again. Like I've said to you, Mr. Chairman, and to our committee members, when you deal with integrity and transparency, it's like money in the bank.

Mr. CUMMINGS. And so I would just ask you to just work with us and see what we can come up with. That's all.

Chairman CHAFFETZ. My last point. My last point. I don't think it's appropriate. I disagree with the attack on the integrity of the Intelligence Committee. I disagree with that. I think they are of integrity. I think Mr. Schiff and Mr. Nunes are men of integrity and they run that committee appropriately. And I'm sorry you don't feel that way.

Mr. CUMMINGS. I didn't—now, see, now you done put something in my mouth. Let me be real clear. No, no, no, no, no.

Chairman CHAFFETZ. I get to make my point. I'll let you——

Mr. CUMMINGS. No, you said something that's not accurate. What I said was—I'm not questioning the integrity of Mr. Nunes or Mr. Schiff. Mr. Schiff—both of them I have a lot of respect for. What I'm saying is what the gentleman said, is that we want a report—when people look at the situation—I'll be very brief. When people look at the report and they see somebody on the transition team for Mr. Trump, then it becomes questionable. All I'm saying to you as to the world, we want—that's why we filed the bill that we filed. And that's why we're asking for more like an independent investigation. That's all.

Chairman CHAFFETZ. Last point. Last point. Last point. And we're going to recognize Mr. Meadows. We've gone way past the time here.

Mr. CUMMINGS. Thank you.

Chairman CHAFFETZ. And I ask this rhetorically. Do the Democrats truly want this committee to do an investigation of the DNC and the DCCC?

Mr. LYNCH. Yes, we do.

Chairman CHAFFETZ. Wow. Okay. We're now going to recognize——

Mr. LYNCH. A lot of these emails, they're already public. They're already public. They leaked them. We already know what they are, those damaging ones.

Chairman CHAFFETZ. Let's recognize the gentleman from North Carolina, Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman. We're going to refocus on the focus of this hearing. I wish that we would have as much passion that is concerned about the well-being of the 22,000 people that got hacked, the potential security breaches that are there, instead of losing or winning an election. I wish we'd have as much passion about that. Let's start to focus on the real aspects of what we need to be doing.

There are other hacks with the IRS. Let's focus on the hard-working American taxpayers. You know, I'm sick and tired of hearing the repeated talking points over and over again. There is no one who will work in a more bipartisan way to get to the truth than me. But I disapprove of the talking points that continue to get repeated to undermine the credibility of a duly elected President.

Mr. CUMMINGS. Will the gentleman yield?

Mr. MEADOWS. No, I will not.

Let me go into this particular issue. When we're looking at this, you mention that you have 100 percent dual authentication throughout the system. Is that correct?

Ms. MCGETTIGAN. Yes, sir. That's my understanding. Yes, sir.

Mr. MEADOWS. All right. And you're filling some very big shoes. I happen to be a fan of Ms. Cobert. She actually—we come from very different sides of the aisle, but she was always very responsive to this committee and to me personally. And so I want to make sure that we can clarify, perhaps, your testimony. Because the 100 percent dual authentication is really just at the front door. Is it not? Because we have indications from the IG that there is still a whole lot within the system, that if they get in the front door, that only 2 of 46 systems inside would require that. Is that your understanding? You may want to refer—I think the CIO wants to jump in here.

Ms. MCGETTIGAN. I think I will defer to Mr. DeVries.

Mr. DEVRIES. Thank you, sir.

Ms. MCGETTIGAN. Thank you.

Mr. DEVRIES. Sir, we have multifactual authentication in there for the users, the standard users who come onto the network. That is correct, 100 percent to get onto the networks, they require their——

Mr. MEADOWS. But once in——

Mr. DEVRIES. No, once they get in, they are still then authorized—their access is based upon those attributes and their roles of what they're assigned to. So they're not given——

Mr. MEADOWS. So how do you respond to the IG that said only 2 of 46 systems would actually, of the major applications, would require PIV authentication? Is that not accurate?

Mr. DEVRIES. I'd like to go back and look at that. I'll defer to my CISO here, but that is—that does not ring true to how we——

Mr. MEADOWS. Because this isn't my first rodeo. I've been here with a number of folks. In fact, I called for the resignation of the OPM director when there were similar terms that I'm hearing today that give me concern that we're making progress. And I guess, how do we define success? At what point will we have all the major applications? And Mr. Lynch talked about the encryption.

Mr. DEVRIES. Correct.

Mr. MEADOWS. Now, we've been promised encryption over and over and over again. And yet even today, we're not there with—so are all the Social Security numbers encrypted today?

Mr. DEVRIES. No, sir.

Mr. MEADOWS. Okay. When will they be encrypted?

Mr. DEVRIES. But I have——

Mr. MEADOWS. Just timeframe. When will they be encrypted, all the Social Security numbers? I mean, that's basic. I've got encryption better than that on my home computer, and here we are, we have—is it a lack of resources?

Mr. DEVRIES. Sir, it was somewhat due to that and also schedule change here on the mainframe. That's the only one that is—that was delayed. And I've reenergized that one back in there. That is 2017.

Mr. MEADOWS. So when is it going to be done?

Mr. DEVRIES. End of 2017, sir.

Mr. MEADOWS. And so we will have everything encrypted by the end of 2017. Fiscal year?

Mr. DEVRIES. The HVA system, the high value assets, which includes the Social Security numbers and so forth, will be encrypted this year. Yes.

Mr. MEADOWS. All right. In terms of segmentation, how do you segment a legacy system? Either one of you can answer it.

Mr. CHASE. So, again, as a part of our strategy, we looked at all the systems and all the IT system inventories that we had out there. We determined which ones——

Mr. MEADOWS. So are you going from a zero trust?

Mr. CHASE. That's the idea, is to use that zero trust tenet. Absolutely.

Mr. MEADOWS. So you rushed into the fire——

Mr. CHASE. Ran into it, sir.

Mr. MEADOWS. —and so as you ran into the fire, you decided from a zero trust aspect that you're going to look at every single system.

Mr. CHASE. Absolutely.

Mr. MEADOWS. All right. So we can tell all of those employees or potential employees or those who have had their personal life history looked at that by the end of 2017, that you have great assurance that we have the most up-to-date, sophisticated cybersecurity protection that they will ever see and it will be segmented in a way that if somebody gets in the front door, that they won't be able to go through the whole system. Is that correct?

Mr. CHASE. That is correct. And there's also many, many compensating controls that reside in the network. So we have our network analysis tool, we have our data loss prevention tool. We have malware detection tools. And then we actually have a 24/7 security operation center that is on glass watching for those events to come through.

Mr. MEADOWS. I yield back. I thank the chairman.

Chairman CHAFFETZ. I thank the gentleman.

I will now recognize the gentlewoman from Florida, Mrs. Demings, for 5 minutes.

Mrs. DEMINGS. Thank you, Mr. Chairman.

I want to say good morning to all of you and thank you for being here. Before I get into my question, I feel compelled to make this comment. I spent 27 years in law enforcement. I served as the chief of police. So I am very concerned about the issue that we're discussing today. Security breaches of any kind, I believe, deserve every bit of attention and every bit of passion. I've been here a little shy of a month, but what I did not sign up for is what I believe was the blatant disrespect that was displayed to each other by my colleagues. And so I believe if we're going to solve our Nation's problems, civility has to be at the center of it.

And with my question, Director Phalen, last November, the New York Times and other media outlets reported that while meeting with the Prime Minister of Japan, then President-elect Trump allowed his daughter and son-in-law to sit in during all or part of the meeting. In reporting about this meeting, the Times found, and I quote, "That anyone present for such a conversation between two heads of state should, at a minimum, have security clearance. What we do not—we do not know whether President Trump has stopped this practice of allowing family members who do not have security clearances from attending meetings with dignitaries and other foreign officials."

Director, I ask you, what are the security risks for having individuals who do not have the appropriate security clearances present during classified meetings or briefings? Thank you very much.

Mr. PHALEN. Thank you, Representative. Thank you for the question. The determination as to whether an individual has a security clearance is left to the head of the agency with whom they are employed or otherwise contracted with. And, of course, the situation between a President-elect and the President is a different situation. The President has the ability to grant a clearance or grant access to classified information to anyone who they please. It is at their discretion.

And the—I am not aware of any of the details around the meeting that occurred with the leadership of Japan. I just don't know any of the details about that, whether anything of classified nature was discussed or not. But it would—in the current situation, it would be the President's discretion to allow individuals even without clearances to know or have access to classified information.

Mrs. DEMINGS. So each department would make that determination. Is that what you said? There are no basic general guidelines for persons to have security clearances in certain situations or positions?

Mr. PHALEN. There are general guidelines and there are—specifically, there are investigative standards which we follow when conducting an investigation. The agency who ultimately grants the clearance follows an adjudication set of guidelines, what are the key factors that one would look at when making a determination whether this individual is eligible or should be eligible to receive classified information. And then as a separate act, the agency then—if the answer's affirmative, they are eligible, the agency would make a determination as to whether to actually brief them into a national security program or not, give them that clearance.

Mrs. DEMINGS. Okay. Thank you very much.

Chairman CHAFFETZ. Does the gentlewoman——
Mr. CONNOLLY. Would——
Chairman CHAFFETZ. Does the gentlewoman yield back?
Mr. CONNOLLY. Would my friend yield?
Mrs. DEMINGS. I yield. I'm sorry. Thank you. I yield.
Chairman CHAFFETZ. She's yielding. To Mr. Connolly or——
Mr. CONNOLLY. To Mr. Cummings.
Ms. DEMINGS. To Mr. Cummings.
Mr. CUMMINGS. I just wanted to let Mr. Meadows know, when I asked you to yield, the only thing I was going to say is before you got here, and I will share this with you, in my opening statement, I talked about all the efforts that we have made in this committee with regard to the other breaches. I listed them one by one, all the many things that we've done. And I said it in a way that—because President Trump has said that we suddenly got excited about the Russian hacking. But I laid it out. And again, I will share my opening—it was a courtesy to you, because I didn't want anybody to think that this is something new to us.

We've spent, in a bipartisan way, hours upon hours upon hours upon hours trying to deal with these. And I give the credit—give a lot of credit to the chairman. And that's all I was tying to tell you.

Mr. MEADOWS. Will the gentleman yield?
Mr. CUMMINGS. And I didn't want the public to be left with the impression that we haven't been working on these acts. Every single time.
Mr. MEADOWS. Will the gentlemen yield?
Mr. CUMMINGS. Of course. I only have——
Chairman CHAFFETZ. It's the gentlewoman's time.
Mr. MEADOWS. Will the gentlewoman yield for just a comment? A nice comment.
Mrs. DEMINGS. Yes. Yes. Certainly. Please, Mr. Meadows.
Mr. CONNOLLY. We'll be the judge of that.
Mr. MEADOWS. The gentleman from Maryland is a good friend, and a trusted one. And in the passion of my not yielding back to him, I don't want anything to be inferred about our relationship and our willingness to work in a bipartisan way. And I apologize for my passion in not yielding. But I also want to stress that our friendship and our willingness to get to the bottom line of it is unyielding and unchanging. And I thank the gentlewoman.
Chairman CHAFFETZ. The gentlewoman yields back.

We'll now recognize the gentleman from Ohio, Mr. Jordan, for 5 minutes.

Mr. JORDAN. I thank the chairman.

Mr. Halvorsen, you are the chief information officer for the entire Department of Defense?

Mr. HALVORSEN. That is correct.

Mr. JORDAN. And in your testimony, your written testimony, you said that, "DOD CIO is responsible for all matters relating to the Department of Defense information enterprise, including cybersecurity for the Department. In this capacity, DOD CIO is responsible for oversight of the Department's efforts to design, build, operate, secure, defend a new IT system to support the background investigative processes for the NBIB." Is that all accurate?

Mr. HALVORSEN. It is.

Mr. JORDAN. Okay. Are you familiar, then, with the December 6 Washington Post story, front page, Pentagon Hid Study Revealing $125 Billion in Waste? Are you familiar with that article?

Mr. HALVORSEN. I am familiar with that article.

Mr. JORDAN. Do you—well, let me ask you—let me go back and ask you this: Do you have the resources you need to do everything I just read in your testimony, help NBIB which has 100 Federal agencies that's got to make decisions about—regarding individuals who work there and everything at the Department, do you have the resources you need to do your job?

Mr. HALVORSEN. We have the resources to make sure that we develop and design an NBIB new system that is secure and can attack and defend the data.

Mr. JORDAN. And so you think you got adequate resources to do everything you're tasked to do.

Mr. HALVORSEN. I think I have adequate resources to everything I'm tasked to do specific to this NBIB issue.

Mr. JORDAN. But not overall? Is that what you're saying?

Mr. HALVORSEN. Well, I don't think anybody here would say they have all of the resources——

Mr. JORDAN. You always want more. I get that. But you are familiar with the story that was on the front page of the Washington Post last month, or 2 months ago?

Mr. HALVORSEN. I am.

Mr. JORDAN. And the findings of the McKinsey & Company study, $125 billion in waste at the Pentagon, do you agree with that—those findings? Or, I mean, they talked about as many full-time employees in back office personnel and in purchasing bureaucracy, as many employees there as we actually have—almost as many people there as we have in troops in the field or troops in total. Do you agree with what you know about that study?

Mr. HALVORSEN. We were—do I personally agree with that study? I do not. Is that the reason I'm here to testify? No. So if you want more data on that, I will take any questions you have for the record.

Mr. JORDAN. Okay. Were you—were you interviewed or talked to in the course of the study by McKinsey & Company? Did they talk to you?

Mr. HALVORSEN. I have talked to McKinsey & Company, yes.

Mr. JORDAN. Multiple times? I mean, I'm just kind of curious.

Mr. HALVORSEN. For the study, I believe once. But I'll get that confirmed. But I have talked to McKinsey in the course of my business.

Mr. JORDAN. The article reports here on the front page here above the fold, the report issued in January 2015 identified a, quote, "clear path for the Defense Department to save $125 billion over 5 years." I think this is important too. What the study said, what the article reports that the study said was that this savings in bureaucracy waste and other areas is money that could go into weapon systems and our troops. Frankly, where I think most Americans would want their tax dollars and resources to go.

The article continues, "The plan would not have required layoffs of civil servants or reductions in military personnel. Instead it

would have streamlined the bureaucracy through attrition and early retirements, curtailed high priced contractors," and the last clause says, "and made better use of information technology."

Do you have any idea what they're referring to there, make better use of information technology?

Mr. HALVORSEN. Yeah, I do. I mean, if you're asking me do we think we could do better with information technology, I think I testified in numerous hearings that do I believe we should continue to adopt best commercial practices? Should we bring more commercial systems on into DOD and other government? I said we should. I believe there are ways to reduce some money in our IT business. Do I think that number is correct, personally? I do not.

Mr. JORDAN. So a little bit ago you said you didn't agree with the study. Now you sound like you do agree with a lot of parts of the study.

Mr. HALVORSEN. No.

Mr. JORDAN. Is it both or——

Mr. HALVORSEN. No. I said I agree that there are efficiencies to be found in the IT systems. By doing what we are doing, I think we will achieve some. I do not think the numbers in the study, my personal opinion, they're not correct. I will take any more questions you have——

Mr. JORDAN. So you think the $125 billion number is a little high. Would you hazard a guess at what kind of savings taxpayers could see if part of what McKinsey found in their study was implemented and how we could better get money to weapon systems and to troops?

Mr. HALVORSEN. No, I will not hazard a guess.

Mr. JORDAN. Okay. Mr. Chairman, I just think this is an important area where we need to—I know it's not the sole focus of and not the primary focus, I should say, of this hearing today, but this is an area we need to study. If we can get more money into upgraded weapon systems and to our troops, and if we got this potential of waste, even the chief information officer says there's some waste there. Maybe not to the degree that the article reports, but certainly any we can find and savings we can find I think makes sense.

With that I yield back.

Chairman CHAFFETZ. Thank you. Point well taken.

I now recognize the gentleman from Maryland, Mr. Raskin, for 5 minutes.

Mr. RASKIN. Mr. Chairman, thank you very much.

I wanted to start actually by responding, Mr. Chairman, to the question that you posed about whether or not the Democratic National Committee would be a proper object for inquiry and investigation by this committee. And my first reaction to it, I think, was sympathetic to you, which is no, not really, because it's not part of the government. It's a private entity for most purposes. When you think about the Democratic National Convention, where it's going to be located, who's going to speak at it, that's a private matter. It's a private association.

On the other hand, it struck me that the Supreme Court has said that political parties are public instrumentalities capable of State action for certain purposes. So when you go back and look at Smith

v. Allwright, Terry v. Adams, the white primary line of cases, the Supreme Court said a political party could not exclude from participation people based on race. So the Equal Protection Clause applied directly to political parties, that they were not private entities for those purposes. They were public instrumentalities.

And in lots of other cases, the Supreme Court has treated political parties as public instrumentalities and kind of public carriers for the purposes of effective action in democracy. And I think if you look at it from a global perspective, that is the role that political parties play. The DNC, the RNC, they are organizing political activity for tens or hundreds of millions of people. And so if they are cyber vulnerable, I think it makes the whole country cyber vulnerable, and then it casts a cloud over democratic government itself.

So that's why, in the end, I think it is a complicated question you raise, but I would side with the ranking member and with the other members who were speaking on this side of it.

Let me pose a question. As a new member of this committee who was—I was not here for the original OPM breach, and so all of this is a bit new to me. But I want to ask the question. We know from the national intelligence community about the fact that they believed with high confidence that there was an organized campaign by Russia to subvert the 2016 election and to compromise the 2016 election. I've also heard that there's certain other countries where certain kinds of hacking are common or concentrated, like Nigeria, apparently, is a place where there's a lot of cyber hacking and phishing attacks going on.

Do you have a list of the most common enemies or culprits of our cybersecurity that you use? And I know, Ms. McGettigan, if that's something you can answer.

Ms. MCGETTIGAN. I'll defer to Mr. DeVries to answer that.

Mr. DEVRIES. Member, if I could——

Mr. RASKIN. Please.

Mr. DEVRIES. If I could, I would like to defer to Mr. Chase here for the expertise on it. We do have the network monitoring, but we are part of the greater ecosystem of that from DHS.

Mr. RASKIN. All right. Let's cut to the chase.

Mr. CHASE. Thank you. No pun intended.

So one of the things that I just want to make clear is we're a customer service oriented agency. And so we rely on our partners from Department of Homeland Security, FBI, and other components within DOD. The potential attribution or the knowing of a bad actor is not our job. My job is to focus the staff at OPM to protect the data that resides in there.

Mr. RASKIN. Okay. So I guess—right. You're a customer service agency and you want to serve the various government agencies that interact with you. The problem, of course, is now we've got these outside entities that are trying to invade and undermine and so on. Do we know who those entities are? Is there like an FBI most wanted list of the cyber saboteurs all over the world or in this country? I mean, the national intelligence community tells us it's Russia, but then we hear from other people, no, it's a fat guy on a couch someplace. I don't know why it's always a fat guy. Why couldn't it be a skinny guy on a couch. But anyway, it might be a guy on a couch or it might be Russia, but it might be Nigeria.

Where it is coming from? And does that list exist? And is there any attempt to really get to the bottom of it?

Mr. CHASE. And, again, I'll try to answer more directly. So DHS and FBI provide those reports in unclassified and classified formats.

Mr. RASKIN. Okay. Do you believe as experts in the field that there is going to be a technological answer to this so we can actually create a secure cyber environment? Or, you know, is this a Sisyphean task? We go up two steps and we fall back three steps. I mean, are we really—is it an uphill fight, I guess is what I'm asking. Mr. Halvorsen.

Mr. HALVORSEN. Right now it is an uphill fight. I do believe technology will get us some of the solutions. But I think this is much like any area in technology. We will make strides forward. The people who want to use technology for bad will make strides forward. And it will be a continuing analysis and engagement that is not going to end anytime soon.

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

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize Mr. Comer who's new to our committee. We're pleased to have him here. The gentleman from Kentucky.

Mr. COMER. Thank you, Mr. Chairman.

Chairman CHAFFETZ. Sorry. The microphone button there. Talk button. There we go.

Mr. COMER. Thank you, Mr. Chairman.

My question is for Mr. DeVries. Sir, I would like to follow up with you on the IT infrastructure project that OPM abandoned last year. The committee's understanding is that you are no longer leasing two new data centers for OPM's new IT environment, but rather, are repurposing the hardware and equipment meant for the IT environment that the contractor Imperatis built. My question is, is this accurate?

Mr. DEVRIES. Yes, sir it is.

Mr. COMER. Okay. How much did OPM pay the contractor for the new IT infrastructure project before terminating the contract May 2016?

Mr. DEVRIES. Sir, I would have to get back to you with the exact amount that was consumed there. I do not have that number with me today here.

Mr. COMER. Why was the contract terminated?

Mr. DEVRIES. Sir, as I completed my assessments coming on board as the CIO, that effort was to build a new infrastructure to move the legacy stuff into. They went out on the contract. That contractor went out of business. They did not show up to work in May, and we terminated the contract after that. We then repositioned the equipment back in because we had purchased that, as we had purchased the design and engineering diagrams. We have what we paid for. Now just turning it back on.

Mr. COMER. It's my understanding that the first two phases of that were completed, and after approximately $45 million of investment, OPM abandoned the project. But you say that we have what we paid for or did we lose what we paid for?

Mr. DEVRIES. Sir, we have evolved that, and I'm now building on that capability that we purchased then. Yes, sir.

Mr. COMER. So is OPM still operating the legacy IT environment? Is that correct?

Mr. DEVRIES. Sir, I will say no. We have evolved a lot over the past year, and that was part of my assessment coming onboard was to take a look at what the network was, where are our high value assets, where are our centers of gravity, if you will, and what's the protection there. Mr. Chase has talked about some of the defense and depth that we've put in place. So it is not the same legacy infrastructure that it was in 2015. Not by a long shot.

Mr. COMER. So are we—can we be assured that this environment is more secure today than prior to the data breaches?

Mr. DEVRIES. Absolutely. Mr. Chase and I would not be here if it was not.

Mr. COMER. Okay. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentlewoman from the Virgin Islands, Ms. Plaskett, for 5 minutes.

Ms. PLASKETT. Thank you, Mr. Chairman. And thank you all for being here this morning to testify.

I wanted to—I appreciated your testimony this morning on all of the topics. And it seems to be very wide ranging, of the discussion that we're having this morning. But we are all here because protecting our Nation's security from insider threats and external threats is of paramount importance, of course, to you all and us as Members of Congress. So I wanted to discuss the security clearance process and how individuals are granted access to sensitive information.

Director Phalen, for you specifically, how would NBIB handle the clearance process for someone under active FBI investigation? What happens with that application?

Mr. PHALEN. When an agency puts an individual in for a clearance, it starts with a determination by that agency that this individual needs a clearance for whatever work they're going to be doing. The individual's information is sent to NBIB or to some other——

Ms. PLASKETT. And what if you find out that the person is under active FBI investigation? What happens at that point?

Mr. PHALEN. If we in the process of conducting the investigation determine an individual's under active investigation, we would notify the requester of what we understand to be the investigation, and we would continue the—our part of the investigation, unless we were told to stop based on some decision by the requester.

Ms. PLASKETT. Now, in knowing that you're going to continue the investigation of someone who is under an active FBI investigation, would that be one of the factors in disqualifying an individual from a security clearance?

Mr. PHALEN. Not necessarily. And it would not be our determination. It would be the determination of the requesting agency, who is either the requesting agent themselves, if they have independent adjudication authority, or the—in the DOD world, the consolidated adjudication facility. These are the individuals that make the ultimate determination as to whether an individual is eligible for access to——

Ms. PLASKETT. Got you. So you're processing the application, you're giving them the information, and then the agency head then makes the determination whether or not the person has the security clearance?

Mr. PHALEN. Ultimately, yes.

Ms. PLASKETT. So for the ultimate decisionmaker for granting a security clearance for a senior White House staffer, who would that person be?

Mr. PHALEN. The chief of the White House Security Office is the adjudication authority.

Ms. PLASKETT. And so the chief of the security office for the White House is the determiner for an individual in the senior White House level having a security clearance.

Mr. PHALEN. Yes.

Ms. PLASKETT. And who places that person in that office? The chief officer. Is that an independent? Is that appointed by the President? Is that a career person? Who is that individual?

Mr. PHALEN. I actually don't know right now. I can find that answer——

Ms. PLASKETT. I would really love to know that answer. Because is it possible for the ultimate decisionmaker to make a decision to grant an individual a national security clearance if the person is under an FBI investigation? You're saying yes, that's possible.

Mr. PHALEN. It is possible.

Ms. PLASKETT. And the reason I'm asking that is because of course—you know, of course there's a reason I'm asking. Right? There would—according to multiple reports, several members of the Trump campaign and incoming Trump administration may currently be under FBI investigation for their connections with the Russians; the very country implicated in the hacking that everyone seems to be interested in here today.

So President Trump's National Security Adviser, Michael Flynn, is reportedly being investigated by the FBI for phone calls with a Russian diplomat. And the New York Times reported that the FBI's investigating communication and financial transactions between Russia and the former campaign manager, Paul Manafort.

So my question is, if these individuals become now senior White House staffers who need security clearance as having sit on this National Security Council, along with Steve Bannon, if those individuals are under FBI investigation, they may still get a national security clearance?

Mr. PHALEN. That is certainly possibly. And I would distinguish between someone who is under investigation and someone who has been charged or convicted with a crime.

Ms. PLASKETT. Of course. As a lawyer, I know you're innocent until proven guilty. But an active FBI investigation would raise some eyebrows. Would it not? Because the FBI would not begin an investigation on my, you know, freshman student who has cheated on a test or something. They usually start FBI investigations for pretty serious things.

Mr. PHALEN. It would be a noteworthy item on an adjudication, yes.

Ms. PLASKETT. Okay. Mr. Chairman, I think we need the answer to some of the questions that we've been asking here.

And so do you know, Director Phalen, which or any of the senior White House staffers who have access to senior material are under criminal investigation by the FBI?

Mr. PHALEN. I do not know that, no.

Ms. PLASKETT. Okay. Thank you.

Chairman CHAFFETZ. If the gentlewoman yields back, Ms. McGettigan, she is the acting director of OPM, if you could get back to Ms. Plaskett about who specifically is in charge, I think the gentlewoman asked a reasonable question here, who are the people that make those determinations, and get back to—will you make that commitment——

Ms. MCGETTIGAN. Yes, we will.

Chairman CHAFFETZ. —that you'll get back to her?

Ms. MCGETTIGAN. We will get back to you.

Chairman CHAFFETZ. Okay.

Ms. PLASKETT. Thank you. Thank you very much, Mr. Chairman. As well if you would find out how do we find out——

Chairman CHAFFETZ. Ask her.

Ms. PLASKETT. It would be great to know in that process, one, who the decisionmaker is, and is there a list of individuals who are under FBI investigation. If the chairman and the ranking member would receive that, that would be very helpful in making that determination, what are the factors.

Ms. MCGETTIGAN. Okay.

Ms. PLASKETT. Thank you.

Ms. MCGETTIGAN. We will follow up. Thank you.

Chairman CHAFFETZ. And I would open up to any member, if they have questions for OPM, Ms. McGettigan is the acting director.

Mr. CONNOLLY. Mr. Chairman, I just—I assume at some point Ms. McGettigan's going to actually answer a question as opposed to always getting back to us.

Chairman CHAFFETZ. Okay. She wasn't ever even asked a question in that series, so I think that's a little inappropriate. But let me—and she did make a commitment to get back to the committee. I think that's reasonable.

Mr. CONNOLLY. Yes, I heard.

Chairman CHAFFETZ. So I'll now recognize myself for 5 minutes.

And I guess this question will go to Mr. Chase. Tell me about the authority to operate. There have been some questions about this in the past. The inspector general found that the authorities to operate were a material weakness in fiscal year 2016. The IG reported that 18 major systems still did not have current authorities to operate in place. What is the current state of those ATOs?

Mr. CHASE. So all the ATOs——

Chairman CHAFFETZ. If you can move that microphone a little closer. I apologize, sir.

Mr. CHASE. So all the ATOs are currently compliant.

Chairman CHAFFETZ. Can you put some meat on the bones? Define that for us.

Mr. CHASE. So in fiscal year 2016, again, our strategy was to identify and understand all the systems. It was identified that quite a few of them were out of compliance. So we took on two major initiatives at OPM. One was a sprint in February of 2016 to

look at all the systems, to include the HVAs, to ensure the best pathway forward to get them compliant. The next phase of that was marketing within OPM and the agency heads and the acting director at the time to ensure that everybody in the agency knew the importance to get everybody into compliance.

Chairman CHAFFETZ. Would the ATO—you said all of them. Would that include the PIPs?

Mr. CHASE. That is correct, sir.

Chairman CHAFFETZ. It would. Okay.

Mr. CHASE. That was not reflected in the fiscal year 2016 FISMA report, and has been recently.

Chairman CHAFFETZ. Everything within the NBIB, do those all have current valid ATOs?

Mr. CHASE. Yes, sir.

Chairman CHAFFETZ. Okay. Let me switch over here, if we could, to Ms. McGettigan and—or maybe, Mr. Phalen, you might be the right person—actually, let me ask you, Mr. Phalen. What is the current state of the ability to look at the social media? We've been talking in this committee over the last couple of years, actually, with OPM about during background check investigations looking at social media. What are you doing or not doing in that process?

Mr. PHALEN. Thank you, Mr. Chairman. Two points to make on that. Number one, in April of 2016, the security executive agent sent out a directive that would allow us—allow an investigation to use social media publicly available on electronic information in order to inform an investigation. We at NBIB or its predecessor, the Federal Investigative Service, have been using on a targeted basis social media inquiries to help resolve issues when they come up during an investigation. We are in the middle of a short pilot to understand how we can incorporate it into a formal—into a more consistent use during an investigation.

In other words, how do we collect the information, get it disambiguated, and make sure it is accurate and of any value, and then provide it to an investigator who is in the field conducting an investigation to help enhance that.

Chairman CHAFFETZ. Can you define "short pilot?" Because I think we've been talking about this for a couple years. And this doesn't seem to be very short.

Mr. PHALEN. So a number of pilots have been conducted by a number of agencies to look at the value of social media. And most concluded—most have reached the similar conclusion, there can be valuable information in collecting social media.

Chairman CHAFFETZ. Okay. Can you just hold on here. This is what drives people crazy about government. You had to conduct a study to find out if looking at social media would be valuable? And the conclusion is it might be yes? Come on. Every single time there's a terrorist attack, what's the very first thing the investigative body does? They go look at their social media. And more often than not, they say, oh, my goodness. If somebody had just looked at this.

Why in the world do we need—we're still doing a pilot? Let me answer the question for you. Yes. Looking at publicly available social media should be part of the background check. It's a joke to think that you're not looking at social media. And the idea that we

even have to think about this, by its very definition, it is social. It is open. It's there. Facebook. You can go—come on. Instagram. Twitter. Every single time we go and do an interview for somebody, we go check their social media. Why do you have to do another pilot?

Mr. PHALEN. The pilot was not to determine whether or not there's any value in social media. The pilot that we are currently running is how do we incorporate it into a standard background investigative process. And the largest pole in this tent here is not can we collect the information. It is not is there going to be valuable information in there. It becomes how does it get incorporated in a manner that is cost effective to our customer base. And—because the collection is the easy part. The analysis of it becomes harder. And the more data that's out there, the more difficult the analysis becomes.

I believe that this is a relevant data source. We believe it is a relevant data source. We're going to continue to exploit it. This pilot was a very short one to determine how we can build it into an—our current investigative process. And as we move down the road, how it will become more of a mainstay for this investigative process.

Chairman CHAFFETZ. Have you considered implementing a policy to require the disclosure of online user names or social media identities as part of the clearance process?

Mr. PHALEN. We have not at this point.

Chairman CHAFFETZ. Why not?

Mr. PHALEN. That would be a decision to be made by the security executive agent to ask for that information.

Chairman CHAFFETZ. Here's my personal take on this, and then we'll go to Mr. Connolly. The United States of America, the people of the United States of America, are about to entrust somebody with a security clearance that allows that individual to look at and understand information that the rest of the public doesn't get to look at. Right? That is the very nature of a security clearance. We're doing this, we're giving this person special privileges because we trust them.

I would think it would be reasonable that in return for that—you don't have to apply or try to get a job with a security clearance. There's nobody that forces you to do that. It's optional. But you would think in return for that they would say: Yes. Here's my Instagram account. And I would go so far to say: Here's my password if you want to go look at my private Instagram. That is a reasonable thing to look at when you're trying to go back and do a background check.

Some of these background checks are so thorough. You're looking at bank records. You're looking at education. You're interviewing neighbors. You're talking and trying to figure out as much as you can about this information. A very costly, expensive, laborious process. And yet we're not even—we're so bashful we won't even say: We're going to be looking at your Instagram. Is that okay, you know? And if it's not, then maybe we shouldn't be giving them a security clearance. That's my take on it.

It's very frustrating this takes so long. Because every time we have a problem, what's the very first thing the FBI and other law

enforcement want to do? They want to dive into their social media. That's the best way for them to figure out what has been going, what is the attitude, who are they communicating with. And if we're going to give a security clearance, it seems reasonable.

I'm past my time. I'll now recognize the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. I thank the chair. I also would say to the chair, I caution him, I don't think it's appropriate for him to characterize an intervention or a question by a member of this committee. I don't do that to him. And I expect him not to do it to me. And if we're going to get into that, two can play the game.

Ms. McGettigan, a question maybe you can answer. OPM, is it going to migrate to the required XML format, the transaction submissions and background checks instead of using legacy systems? I thought I heard Mr. DeVries say we're pretty much done with the legacy systems. Have we fully migrated to the required XML system?

Ms. MCGETTIGAN. I will have to defer that to Mr. DeVries.

Mr. CONNOLLY. You don't know the answer?

Ms. MCGETTIGAN. I do not.

Mr. CONNOLLY. Mr. DeVries.

Mr. DEVRIES. No, sir, we have not.

Mr. CONNOLLY. Why not?

Mr. DEVRIES. So the whole legacy system is comprised of eight different systems which ask questions and interact and portray in conducting the investigation through them. A lot of the language on, especially I think it was a member here brought up the word PIPs, which is the main database system that maintains it there, that is on—written in language that is no longer supported. And I'm trying to move it out of there.

It is not just merely a case of just taking something and putting it out to XML. We have employed XML in terms of the interface going into the customer. We have put that into all their front-facing applications there. And in that time, we've also put other protections in there, like masking of the Social Security number and other techniques. So yes, to the customer facing one, as we have on other OPM systems, we have put the XML piece into it.

Mr. CONNOLLY. Ms. McGettigan, what is OPM and NBIB doing to ensure that if data is exfiltrated from the NBIB, NBIS systems, that the data will be protected and its location and attempted use not—will not only be prevented but visible to the NBIS for action? What are you doing to protect that in the exfiltration process?

Ms. MCGETTIGAN. Again, sir, I'll——

Mr. CONNOLLY. Can't hear you.

Ms. MCGETTIGAN. I apologize. Again, sir, I will have to defer to Mr. DeVries or Mr. Halvorsen.

Mr. CONNOLLY. So again you can't answer the question.

Mr. DeVries.

Ms. MCGETTIGAN. I cannot.

Mr. CONNOLLY. Does the acting director of OPM get involved in these cyber issues at all?

Ms. MCGETTIGAN. I do get involved somewhat, but not in the details.

Mr. CONNOLLY. Have you had any experience with the breach or responding to the breach in your period of time under Beth Cobert or Ms. Archuleta before that?

Ms. MCGETTIGAN. I—when the breach occurred, I was in another area of the organization. I was in Human Resource Solutions. I was not the chief management officer at that time, so I was not intimately involved. I was involved from another area of the—I had no responsibility for that.

Mr. CONNOLLY. Mr. DeVries, what are we doing about that exfiltration, protecting that data so it's not breached?

Mr. DEVRIES. Yes, sir. Sir, on a macro prospective, let's start with the worthy employee or the individual who's going to be investigated. He enters his records or his information into the e-QIP through the SF—Standard Form 86. That information is stored securely. It's on an encrypted database. That is what gets queued up to go to the investigators once they are awarded that work, if you will, from the NBIB. With my coming on board in September, we changed that process.

In the past, when the companies would get their task orders to do these investigations, and we just talked about the contract that was awarded out to the four new companies, two of those were existing ones and there are two new ones in there, the investigators no longer can download that information to their company information stores. It stays as part of the government, and we've incorporated a new security thing there where when they pull the records in, it is on a different encrypted system under their hard drive, and they authenticate themselves with a verification card that is issued by OPM and NBIB to them.

Mr. CONNOLLY. I only have 30-something seconds, so let me ask another question. What are we doing to boost the capacity to decrease the enormous backlog on security background checks? Mr. Phalen.

Mr. PHALEN. Yes, sir. We have done two things of large proportion. Number one, as was referenced earlier, we have started a new contract period and doubled the number of companies that are available to provide the contract investigations. And that, we believe, will have a significant impact on our ability to work off the backlog. At the same time, in fiscal 2016, we hired 400 new Federal investigators into the service. And we plan on, in 2017, adding another 200. And we are already seeing the fruits of that addition to work off the capacity.

Mr. CONNOLLY. I think this is on top of many topics we're talking about. This is really important. I get complaints all the time, especially from private sector companies with enormous numbers of jobs at the ready they cannot fill because of this backlog. And so the more we can do to streamline, expedite, while making sure it's still accurate, I think is really critical moving forward.

Thank you.

Mr. PHALEN. Yes, sir. I agree.

Mr. CONNOLLY. I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from Alabama, Mr. Palmer.

Mr. PALMER. Thank you, Mr. Chairman.

I know you're new on the job, Ms. McGettigan, and if there's anyone on the panel who can answer this, I'd appreciate it. Does OPM allow employees to access personal email accounts, Facebook, do any other personal business using the Federal server?

Ms. MCGETTIGAN. Employees are allowed to do limited access for personal and business. Access their bank accounts, what have you. So there's limited access for personal business. Limited use.

Mr. PALMER. Are you aware that it was reported that the Immigration and Customs Enforcement agency just a couple of years ago, I think it preceded maybe by a year or so the breach of the data systems at OPM, they had numerous cases where the breaches were coming—or the attacks were coming through the use of personal email utilizing the Federal server? Are you aware of that?

Ms. MCGETTIGAN. No, sir, I was not.

Mr. PALMER. Well, it's an area that concerns me where—and employees, and not only employees, but high ranking officials, and I don't know that you could answer this, if there are any OPM directors or other high-ranking officials using personal email accounts—or accessing personal accounts using the Federal server or using personal accounts to do business. We know that's been a problem in other agencies, most notably the State Department.

One of the things that concerns me is that it doesn't appear to me that we've made the maximum effort to protect ourselves from cyber intrusion. And for the record, I'd like to point out that James Clapper made the point, the Director of National Intelligence, that it was the Chinese, not the Russians, that we believe hacked OPM. But I think this may have been asked earlier.

OPM is still not fully compliant with the requirements for the use of personally identifiable verification cards, the PIV cards. Where are we on that?

Mr. DEVRIES. Sir, I'll take that. Sir, we are 100 percent compliant for the PIV cards for the users to access the network.

Mr. PALMER. So is it a chip-based card?

Mr. DEVRIES. Yes, sir, it is.

Mr. PALMER. And multifactor verification?

Mr. DEVRIES. Multifactor verification.

Mr. PALMER. So we've got that across the board?

Mr. DEVRIES. It needs the card and then you need the personal identification that you put your PIN in for. Correct, sir.

Mr. PALMER. Let me ask you this: In regard to hiring people who handle your data systems, and particularly to protect against cyber attacks, how long does it take to process an applicant? For instance, I've got a—there's a gentleman in—at the University of Alabama, Birmingham, one of the top people in the country on this, Gary Warner, and he's turning out some of the best experts in cybersecurity. And the day they graduate—it's almost the day they graduate, they can get a job with Visa, MasterCard. But it seems to take months to even get in the system for the Federal Government. Is that an issue at OPM?

Ms. MCGETTIGAN. Well, yes, sir, it is an issue in terms of the background investigations. We are very much backlogged. We are committed to reducing that backlog. And we have—to that end, we have just—we have just awarded contracts to increase our capacity,

the field contracts to increase our capacity. And we are on a path to reduce that—to reduce that backlog. But it will take time, and employees of OPM or prospective employees of OPM are also waiting for background investigations.

Mr. PALMER. Well, I know that—and I wasn't here for the opening of this hearing—that there seems to be a tendency to try to make this—politicize this. And if that's where some members want to go with it, that's fine. But I think the seriousness of the breach at OPM requires that we do our jobs to make sure that our data systems are secure.

And one of the things that I might suggest and encourage you to consider is doing the background checks on these top students while they're still in school so that when they graduate, we're not going to lose them to the private sector. I think that we put ourselves at great exposure by not having quicker access to the best people that are available to protect our data systems.

Is that something that OPM might consider? Could we expedite the process? Because it's unreasonable to think that someone could get a really good job somewhere else and then have to wait months to get an interview.

Ms. MCGETTIGAN. Yes, sir. We do have some programs. We have a program, Presidential Management Fellow Program, where we have people apply—recent graduates apply. And they are vetted and then they become finalists. We do not do—to my knowledge, background investigations are always done at the—once the person receives a conditional offer of employment. So it's the offer of employment that triggers the background investigation.

Mr. PALMER. Well, I thank you for coming today.

And I just want to make this last point, Mr. Chairman, that I think the point that needs to be made is that the purpose of this hearing is to make sure that our data systems are secure. And I think this committee will do whatever we need to do to make that possible.

I yield back.

Chairman CHAFFETZ. I thank the gentleman.

We'll now recognize the gentleman from Wisconsin, Mr. Grothman.

Mr. GROTHMAN. Thank you.

Mr. DeVries, we'll ask you a question again. You know, the GAO recently found——

Chairman CHAFFETZ. Mr. Grothman, my apologies. My apologies. We need to go to the Democratic first. Mrs. Lawrence. I failed to recognize her. The gentlewoman is recognized for 5 minutes.

Mrs. LAWRENCE. I know you would never purposely not recognize me, Mr. Chairman.

Yesterday, Ranking Member Cummings sent a letter to the Defense Secretary about potentially serious violation of the Constitution by Lieutenant Governor Michael Flynn, the President's national security adviser. General Flynn had admitted that he was paid to attend an event sponsored by the Russian-backed television network known as RT. And he dined with the Russian President Putin. RT has been described by the NSA, CIA, and FBI, and I quote: "The Kremlin's principal international propaganda outlet. It

receives funding, staffing, and direction from the Russian Government."

Director Phalen, your staff provided the Standard Form 86 for security clearance holders. One question on the form, and I quote: "Have you or any member of your immediate family in the past 7 years had any contact with a foreign government, its establishment, or its representatives, whether inside or outside of the U.S.?"

My question to you, why are these individuals asked this question?

Mr. PHALEN. Thank you, Representative, for that question. The reason these questions are asked is to ensure that the individual who is making an adjudicative decision understands what relationships an individual may have with a foreign government or foreign representative. And the nature of that question is to get to the heart of what that relationship may be. It could be benign, it could be not benign. But this would be the judgment of the adjudication organization. Our goal would be, based on the response to that question, to gather as much information as we can get to——

Mrs. LAWRENCE. The form also asks the question, and I quote: "Have you in the past 7 years provided advice or support to any individual associated with a foreign business or foreign organization?"

So my question to you is, do you know if General Flynn has a clearance?

Mr. PHALEN. I have not checked the record. I believe he does have a clearance, but I don't know that authoritatively. And if I could add, that the investigation of General Flynn, given his role in the White House, would generally be conducted by the FBI and not by NBIB.

Mrs. LAWRENCE. So you don't know if he has a clearance, correct?

Mr. PHALEN. I don't know authoritatively, but I believe he does.

Mrs. LAWRENCE. Do you know if he ever reported to the appropriate authorities?

Mr. PHALEN. I do not know that.

Mrs. LAWRENCE. Do you know if General Flynn ever reported how much he paid—how much he was paid for his trip?

Mr. PHALEN. I do not know that.

Mrs. LAWRENCE. So you're stating within the government that would be the FBI that would answer that question?

Mr. PHALEN. The—his reporting chain, if his clearance was still through the Department of Defense, would have been back through a Department of Defense security office, and they would be the organization that would have that on the record. It would be up to the FBI, if they were doing the investigation, to go back and reach out to the Department of Defense and ask if that had been reported.

Mrs. LAWRENCE. Do you know if that reach-out has happened?

Mr. PHALEN. I do not know.

Mrs. LAWRENCE. Mr. Chairman, we need to get answers to these basic questions. And I am requesting that the committee send a letter requesting a copy of General Flynn's security clearance application, as well as any and all updates he may have submitted.

Will the chair agree to that?

Chairman CHAFFETZ. Send me the request.

Mrs. LAWRENCE. I appreciate it.

Mrs. LAWRENCE. We have a responsibility, and we have been talking about this. And, Mr. Chairman, you have been a staunch leader in this, and this is an area I feel that we need questions answered. Thank you so much.

Chairman CHAFFETZ. I now recognize the gentleman from Wisconsin, Mr. Grothman.

Mr. GROTHMAN. Okay, Mr. DeVries. GAO found that personnel management had not yet completed and submitted a data center optimization plan. And, originally, that was supposed to be done in September of last year. Do you know when that plan will be completed, or has it been completed?

Mr. DEVRIES. Thank you, sir. I appreciate that question because that's one that's near and dear to my heart.

I came onboard as the CIO in September. We did not publish that one, because it was not complete. I completed the assessment on it, and we're finalizing that. And that should be done back up to OMB by the end of this quarter here.

Mr. GROTHMAN. By the end of?

Mr. DEVRIES. This quarter.

Mr. GROTHMAN. Okay. So the next couple months. Okay. Do you know what the savings goal you have for a plan like that is?

Mr. DEVRIES. Sir, I do not have the savings goal in terms of the final numbers yet. That's part of the assessment that's still ongoing right now.

Mr. GROTHMAN. Okay. How many data centers do you own now?

Mr. DEVRIES. Today, sir, I own seven. We closed down two, and we're about ready to move out of our third one here in the next 2 months.

Mr. GROTHMAN. Oh, that's good. What do we have left? What are the ones that are left?

Mr. DEVRIES. And then I have five left. And I'm going down to two.

Mr. GROTHMAN. Okay. Good.

Let me give you another question. During the data discovery breach and mitigation process, your relationship with the inspector general was strained. There was a lack of communication, time—there wasn't timely reporting, I think the IG wasn't informed really what you would consider on a timely basis. I understand things have improved since that time. How would you characterize your relationship with the inspector general today?

Mr. DEVRIES. On behalf of the CIO office, I'll say it's very good. I say that because we meet monthly with his staff and my staff to go through what their concerns are, what their findings are, what our status is of reporting back to those findings. It's a very good relationship. They hold nothing back.

And I'd like to defer now the final question to my chief information security officer, because he deals with them much more frequently.

Mr. GROTHMAN. Okay.

Mr. CHASE. Is that okay, Representative?

Mr. GROTHMAN. Sure. Yeah.

Mr. CHASE. So one of the things when I came onboard was to establish a good relationship with the inspector general. We meet on

a weekly basis to talk about all the progress. And so—and I know I mentioned it earlier, but I'll say it again, is everything from the compliance efforts that we did to the engineering rollouts, so there's a lot of things going on that I wanted to make sure that the inspector general is abreast of. And so with that, they've given us guidance on what's appropriate to align to their FISMA report metrics and reporting. And it's been helpful not only for me but my staff behind me to see why that relationship is one that pays dividends in the long run.

Mr. GROTHMAN. Good. And if there was a breach today, how quickly would the inspector general know?

Mr. CHASE. As quickly as everybody else.

Mr. GROTHMAN. Okay.

Mr. DEVRIES. Sir, I make that first phone call to the director, the second one is to the OIG, so it's realtime——

Mr. GROTHMAN. Okay. Thank you.

I yield the remainder of my time.

Chairman CHAFFETZ. The gentleman yields back.

I now recognize the ranking member, Mr. Cummings.

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

Director Phalen, according to the website, the National Background Investigations Bureau, NBIB, is now responsible for conducting, and I quote: "Approximately 95 percent of the total background investigations governmentwide."

Is that right?

Mr. PHALEN. Yes, sir, that is.

Mr. CUMMINGS. Out of the total number of background investigations that NBIB is responsible for conducting, does that include political appointees in the Trump administration?

Mr. PHALEN. Generally not.

Mr. CUMMINGS. Not?

Mr. PHALEN. Generally not.

Mr. CUMMINGS. Okay.

Mr. PHALEN. Yes.

Mr. CUMMINGS. And why not?

Mr. PHALEN. By tradition, that work has been given to the FBI to conduct those investigations by the White House.

Mr. CUMMINGS. And so a—now, guideline A of the adjudicative guideline states that individuals seeking a security clearance must have unquestioned allegiance to the United States, and lays out a series of examples of disqualifying factors that investigators and adjudicators will use to determine eligibility.

Based on some of the questions on that SF86, I think many people often think of association with groups seeking to overthrow the U.S. Government by violent means, like violent anarchists or terrorist groups. When we think of this guideline, is that fair?

Mr. PHALEN. Yes, that would be a major piece of that category. Yes, sir.

Mr. CUMMINGS. But the disqualifying factors in the guideline may include much more than that. Do they not? They include whether a person associates with or shares the viewpoint of those who advocate using illegal or unconstitutional means to prevent government personnel from performing their official duties or others from exercising their constitutional rights. Is that correct?

Mr. PHALEN. Those are—those are questions to be considered in an adjudication, yes, sir.

Mr. CUMMINGS. And it could—and it could conclude—include persons who associate or share the viewpoint of those who use illegal or unconstitutional means to, quote, "gain attribution for perceived wrongs caused by Federal, State, or local government," end of quote. Is that correct?

Mr. PHALEN. Those would be adjudicative questions, yes, sir.

Mr. CUMMINGS. If your investigations uncovered negative or derogatory information in any of those areas, I imagine that you could raise concern with regard to them. Is that correct?

Mr. PHALEN. They would be noted in the investigation, and they would be forwarded to an adjudicative—adjudication authority to make a determination as to whether that individual should be cleared.

Mr. CUMMINGS. So I want to walk you through a few short examples. If someone said that they were a Boy Scout or Girl Scout, would that raise a concern under guideline A? Of course not. Is that right?

Mr. PHALEN. No, sir.

Mr. CUMMINGS. What if someone described themselves as a Leninist, which refers to the Russian revolutionary who was not a fan of our democratic government, should that raise concerns for your investigators?

Mr. PHALEN. It would, and the investigator should pursue that avenue of discussion with the subject as to what that means.

Mr. CUMMINGS. What if someone said that his goal was to, quote, "destroy the State," unquote, what response would that elicit?

Mr. PHALEN. That would elicit a very strong line of questioning with that individual and with others to determine what he means by that, so that we can give a full picture to the adjudicator.

Mr. CUMMINGS. What if somebody said, quote, "I want to bring everything crashing down and destroy all of today's establishment," end of quote, should that raise a concern?

Mr. PHALEN. That would be noteworthy in an adjudication, yes, sir.

Mr. CUMMINGS. Chairman, each of these phrases were reportedly used by Steve Bannon to describe his views and his goals, according to Ronald Radosh of The Daily Beast. Mr. Bannon has since reportedly denied saying those things, but I imagine an investigator would still have concerns about them. I imagine that they would also want to see numerous reports about racism rampant on the news website Mr. Bannon used to run.

Mr. Chairman, this is—this is a very serious problem. The President has picked Mr. Bannon to be his chief strategist and senior counselor. Not only that, the President just reorganized the National Security Council and gave Mr. Bannon a permanent seat at the table, while removing the chairman of the Joint Chiefs of Staff and director of National Intelligence. This is at least—I mean, it causes us to—we should wonder about this and question it.

Do you—if—you may have answered this earlier. If somebody is under criminal investigation—and I know that we now have a liaison. Tell me how that works, a criminal liaison to try to work

with—what happens when you find out somebody is under criminal investigation?

Mr. PHALEN. Depending what the criminal—criminal investigation is and the immediate seriousness of the nature, we may immediately contact the requesting agency that is asking for the clearance to give them sort of a heads-up that this is out there. And they may or may not determine at that point they want to terminate the request for a clearance. Otherwise, we'll continue the investigation.

The fact that—going further down the road, an adjudicator would be faced with this question, this is an individual under criminal investigation, it would be up to them to understand what that investigation is about and to make a judgment whether or not that investigation or what is surrounding it would be disqualifying for access to classified information, whether—essentially, whether it shows an inability to be trusted to hold onto classified information.

Mr. CUMMINGS. So, in other words, the person could still get a—get a clearance?

Mr. PHALEN. Yes.

Mr. CUMMINGS. And I would assume that if that person were then later on convicted of an offense, then that probably his clearance would be withdrawn. Is that right?

Mr. PHALEN. If——

Mr. CUMMINGS. And who would do that?

Mr. PHALEN. The organization that issued the clearance would be the organization to rescind the clearance. And—based on what they see. And they would make—and if it had already been issued, an individual is convicted, it would be up to that organization to determine whether or not that conviction has any impact on their ability to be trusted.

Mr. CUMMINGS. My last question. The—I just gave some quotes that are attributed to Mr. Bannon. Would—I mean, if they—if you were to raise—if those questions were raised, would anyone go and then—and then the—say, Mr. Bannon, or whoever may have said those kind of things, denied them, would, then, you—would—would somebody go back to look to see if those statements were made in other—in the periodicals, whatever? And how might that affect the security clearance of that person? Do you understand my question?

Mr. PHALEN. I believe I do. We—if—if we—first, if we were faced with an individual who had made statements that appeared to be counter to the United States, that would be an issue we would pursue with the subject themselves, to start with. And to use your example, if that individual said, no, I never really said that, I don't really feel that way, we would use, to the best of our ability, whatever sources we can find to get to—to do issues resolution, to determine whether—what the truth is, to the extent that we can, so that we can give as full a picture as we can to the official that has to make that ultimate decision.

Mr. CUMMINGS. And if you discovered that, unequivocally, that the person had not been honest with you, what might—effect that have?

Mr. PHALEN. That would, again, be passed on to the adjudication authority, and they would have to determine whether that makes a difference or not.

Mr. CUMMINGS. Mr. Chairman, thank you for your indulgence.

Chairman CHAFFETZ. Thank you.

I'll now recognize the gentlewoman from New York, Mrs. Maloney.

Mrs. MALONEY. Thank you, very much.

Chairman CHAFFETZ. Your microphone. Microphone.

Mrs. MALONEY. You know, I'm really concerned about cybersecurity. And if Congress is serious about helping agencies improve their cybersecurity, it must call on the President to rescind, in my opinion, his across-the-board hiring freeze. How in the world can you move forward if you can't even hire the people that can do the job? Such—this freeze that he's put in place, in my opinion, undermines the Federal Government's ability to recruit, develop, and maintain a pipeline of cybersecurity talent that's needed to strengthen Federal cybersecurity. And if there was a field that didn't change every 24 hours, it's cybersecurity. You have to get the youngest, brightest, latest people that are involved in it.

So I am concerned about this freeze that he put in place, I think it was roughly 2 weeks ago. And he's taken other steps that will make it more difficult for Federal agencies to improve the area of cybersecurity. So I—and then he issued this memoranda ordering across-the-board hiring freeze in the Federal Government. And I want to quote from it. And I quote: "As part of this freeze, no vacant positions existing at noon on January 22, 2017, may be filled, and no new positions may be created."

So it seems to me that when it comes to improving cybersecurity, a hiring freeze is one of the most counterproductive policies that you could ever put in place.

And after the 2015 cybersecurity at OPM, Federal CIO Tony Scott and then OMB Director Shaun Donovan put in place a cybersecurity strategy and implementation plan for the entire government. And I quote: "The vast majority of Federal agencies site a lack of cyber and IT talent as a major resource constraint that impacts their ability to protect information and assets."

And so I'd just like to ask Mr. DeVries, as the CI—CIO of OPM, can you highlight some of the challenges that OPM has faced when it comes to recruiting and hiring cybersecurity specialists? And, obviously, you can't do anything if you can't hire anybody. So could you give us some insights there?

Mr. DEVRIES. Thank you very much for that question. That is a—that is pertained to OPM. It's pertained to the Federal workspace and the Federal cybersecurity and IT professionals. That is a concern to all of us of how do I keep the pipeline coming in there.

I will tell you, from my experience just coming onboard in OPM in September, we have, for example, five hiring actions out there, and we had about a 60 percent—we did not get to them fast enough before they went someplace else. We have completed that. We have filled those things. But, again, that's our challenge across the Federal spaces, how do I recruit and retain these folks.

I will tell you, it comes from the passion of the heart. They come onboard. If I give them meaningful experiences, training they will stay. I think we're also working across the Federal space of how do I help improve the rotation, if you will, from Federal service back to industry and then back in again. We need to make—we

have made strides on it. We need to continue to work on that together.

Mrs. MALONEY. Well, I—I've got to say that cybersecurity is really tied to the security of the Nation. And I think—I don't see how you can do your job if you can't hire people.

So I would respectfully like to request that the chairman think about maybe asking for a waiver for the cybersecurity area in hiring. Number one, as Mr. DeVries pointed out, it's hard to hire them, because they're in great demand all over the country right now, that is a prime focus of the country. And so we need to work in this for the good of the country.

And I—we're all individuals. I'm going to write the President my own letter and request that he waive it for the area of cybersecurity.

But can you just go over some of the agencies, how does this hinder your ability and capability to improve when it comes to securing IT systems when you're not able to hire people? How does this affect you?

Ms. MCGETTIGAN. Congresswoman, it terms of the hiring freeze, this is a 90-day freeze, and there are many exemptions to that freeze, primarily in terms of national security, public health, and public safety.

Mrs. MALONEY. But isn't this national security, cybersecurity?

Ms. MCGETTIGAN. Well, agency heads are able to make that determination and to exempt those positions that are deemed to be national security.

Mrs. MALONEY. So that's taken care of?

Ms. MCGETTIGAN. If they are not—if they have a position, a cybersecurity position, that they would not feel was national security, they can come to OPM and we will review their request for an exemption from that.

Mrs. MALONEY. Have any people asked for exemptions?

Ms. MCGETTIGAN. At this point, no. I'm not aware specifically that anyone has come into OPM. I haven't seen any requests.

Mrs. MALONEY. Okay. My time has expired. Thank you.

Chairman CHAFFETZ. Thank you.

Just a few wrap-up questions.

Mr. DeVries, could you please provide the committee all the NCAPs or other pen test reports conducted in the last year? Is that something you can provide the committee?

Mr. DEVRIES. Yes, sir, we can.

Chairman CHAFFETZ. Okay. Thank you. We appreciate it if you'd do that.

And then, Mr. Phalen, one of the—one of the sad realities of what happened when Director Archuleta was in place is this hack had legacy systems online that dated back to 1985. And my understanding is, even if you applied for a job and didn't get a job with the Federal Government, and you did it after 1985, you might have been in that system.

What are you doing to take sort of the nonactive records so they're not online and, thus, accessible to some hacking? Have you made any adjustments there?

Mr. PHALEN. To be honest, sir, I don't know. I know we have done a tremendous amount, you've heard it earlier today, in secur-

ing the systems. And I'm very comfortable that we have both the barriers on the front end and the ability to, my words, fight sort of an active shooter online on the network, should it appear. I don't believe we've taken a tremendous amount of this and put it offline, because it is—it needs to be accessible for any future work that we do.

Chairman CHAFFETZ. To a degree. I mean, you know, if somebody retired in 1991 and then all of a sudden we have a hack in 2014, it does kind of beg the question why is that system—Mr. Halvorsen looks like he has something.

Mr. HALVORSEN. Yes. The new system will have tiered storage on it both in terms of what's live, what goes back, and it will take into consideration some of the things you said. If you are offline for a while, that will go into a different storage system, and it will be much harder to access.

Chairman CHAFFETZ. It just—it seems like one of the lessons we should have learned for the nonactive employees—again, there may be a period of time. You all are more experts on it than we are, but after a certain amount of time, maybe it should be, you know, more sitting in some mountain somewhere as opposed to online.

Two last questions. Who's in charge? When there's conflict, disagreement, when there is an attack, who ultimately is in charge?

Mr. CHASE. So through my program, we actually have a process that we implemented based on the lessons learned from the 2015 breach, and there is a communication path that routes up into the director's office through the CIO with the severity and any data or details related to that incident.

Chairman CHAFFETZ. So who—who is in charge?

Mr. CHASE. So——

Chairman CHAFFETZ. Who ultimately makes the hard decision if there's a disagreement, a question? You've got the DOD. You've got OPM. Something's not—who is the ultimate decisionmaker?

Mr. DEVRIES. So I'd like to take that on. If it's on the current system that OPM and I, as the CIO, am responsible for, I do that.

Chairman CHAFFETZ. Okay.

Mr. DEVRIES. On the new system, within the NBIS, as we transition to it, DOD will.

Chairman CHAFFETZ. Okay. So that would be Mr. Halvorsen or whoever his replacement is?

Mr. DEVRIES. Correct.

Mr. HALVORSEN. That is correct.

Chairman CHAFFETZ. Okay. Last question. Mr. Halvorsen, you have the freedom of retirement there running around the corner here. So given that, your years of service, your perspective, your expertise, summarize for us, what should the Congress understand? What are your greatest frustrations and concerns and your best suggestions that you can offer us?

Mr. HALVORSEN. Well, first, I'll thank Congress. As you know, working through many of the members here, we did get the cyber accepted service law, which I do think was the first thing that we needed to get done to recruit and move past some of the things that were blocking our ability.

I do think we are going to have to reevaluate the pay scale for cybersecurity personnel and some other key positions. We do rely

on patriotism. We can recruit people a lot for that, but the pay disparities are getting out of hand. I mean, I will tell you, I have lost six or seven people this year, very good, basically, because they could not anymore turn down the offers. And I can't counsel them against that after a certain point.

Chairman CHAFFETZ. I'm totally convinced that you're right. And I hope that this Congress—I plan on helping to champion some legislation to give more realistic assessment to provide that flexibility, because I do think you're right.

Mr. HALVORSEN. And I think the other more most important thing that we do, and I have said this before, I will keep saying it, I do think the secret weapon of our country is, to keep our security, keep our edge in warfighting is better use of our industry and commercial mobility and agility.

You have seen—we talk about this in DOD. We are embarking to bring as much commercial into these activities. We are doing it with this system as the build of the new. We need to continue that, and we need to continue that against—across the foreign government—I mean, across the Federal Government space. That also means we will have to work and raise the bar for industry on security.

While I'll be the first to say that DOD included, we have to get better in our security practices. And I am heartened by what I see in my discussions with the commercial community. They are starting to take that to heed, and we are seeing a rise in their ability to protect data. We need to encourage that and open up our dialogue with the commercial sector on how best to do that and share more information.

Chairman CHAFFETZ. Thank you, again, Mr. Halvorsen. We thank you for your service, and we wish you nothing but the best of luck in whatever your future endeavors take you. And thank you again for your service.

Let me recognize Mr. Cummings, and we'll close the meeting.

Mr. CUMMINGS. Thank you. Thank you. I want to thank all of our witnesses for being here today. You certainly have been extremely helpful. And I want to—you know, I just hope that the—I want to express my appreciation to all the people that work with you, because I know that you all have teams of people who give their blood, their sweat, their tears, because they want America to remain the greatest country in the world.

Mr. Halvorsen, again, I want to join in with the chairman and thank you for your service.

I have a brother who is a former Air Force officer, who is not a cyber expert, so he talks to me all the time about the demand for these folks who are good. I also have sat on the Naval Academy Board of Visitors for the last 12 years. And one thing that we've done in the Naval Academy it's now mandatory that every student have—I know you probably already know this—have extensive cyber lessons as part of our curriculum, and so we see the significance of it.

I want to ask you this: One of the things that we wrestle with is Federal employees feel that they are under attack constantly. We've seen recently where all kinds of measures have been put forth that really make them feel pretty insecure. And I'm just won-

dering, how do you—I mean, first of all, talk about, briefly, the people that you've worked with and what they bring to the table. Because a lot of people, I think, get the impression sometimes that the people who work for the Federal Government are not giving a lot and not giving their best and not feeding their souls, as I often say.

I just want—you know, you're on your way out. You've had an opportunity to work with a lot of people. And I'm sure one of the saddest parts is probably a bittersweet thing, you created a family. I always tell my children that whenever you get a job, you also create a family of people who are looking out for you and who care about you and who you—sometimes you're with more than you're with your own family.

So could you just talk about some of the, just generally, the people that you've worked with, sir? Because I know that you could not have done what you've been able to accomplish without a support system. If you might, just very briefly.

Mr. HALVORSEN. Well, you know, I will tell you, having both been in the military and in Federal service, highest respect for the Federal workforce. They do exceptional work. They put in a lot of hours. They do their best on everything they can do. But I'm also going to comment, I see that also in the commercial workspace when I bring the people in. I do think this is a leadership issue. And if you make your—any of your employees, whether they're Federal, military, or commercial, feel a part of the team and you listen to that team, they will give you everything they've got to get—to get the work done. And that—I have 37 years, that's what I have seen in the Federal Government and in that workspace.

Mr. CUMMINGS. And I think when you show people that you truly care about them—not just about them, but their families and their welfare—I tell the people that come to work with us on the OGR, if they are not better when they leave me, then I've failed. In other words, if they are—their skill level is not higher, if they're not more proficient, if they're not more effective and efficient, then I've done something wrong. Because I want to invest in them. Because I want to be a part of their destiny. I want to touch their futures. Even when I'm dancing with the angels, I want to know that they've gone on to do great things, because our Nation really needs the very, very best.

And so I can tell you that working with the chairman, we saw that. We—in working with the—then I'll be finished. I give the chairman a lot of credit, because when we looked at the Secret Service, he and I made a concerted effort to say to the Secret Service we wanted the elite of the elite. We wanted the very, very best, and we wanted to create that culture.

And I think we're moving toward this, Mr. Chairman. I don't know that we've gotten there yet, but we're trying to get there. But—and we've done that in a number of agencies in a bipartisan way.

And, again, I just—you know, the only reason I raise the question, Mr. Halvorsen, is because I just want the public to be reminded that, you know, there's a vast array of Federal employees that keep our country the great country that it is.

And, again, I want to thank all of you and everybody who back you all up for doing what you do. And, now, we still have a lot of work to do, as you've all made very, very clear, but I believe that, you know, we can—we can get it done.

And thank you, Mr. Chairman.

Chairman CHAFFETZ. Thank you. And thank you all. And please let them know, the men and women who work within your departments and groups, how much we do appreciate it. It's a tough job, but it's a very important job, and we do appreciate it.

Thank you. The committee stands adjourned.

[Whereupon, at 11:28 a.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Statement for the Record

Worldwide Threat Assessment of the US Intelligence Community

Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

February 9, 2016

STATEMENT FOR THE RECORD

WORLDWIDE THREAT ASSESSMENT
of the
US INTELLIGENCE COMMUNITY

February 9, 2016

INTRODUCTION

Chairman McCain, Vice Chairman Reed, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2016 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

The order of the topics presented in this statement does not necessarily indicate the relative importance or magnitude of the threat in the view of the Intelligence Community.

Information available as of February 3, 2016 was used in the preparation of this assessment.

TABLE OF CONTENTS

GLOBAL THREATS

CYBER AND TECHNOLOGY

Strategic Outlook

The consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the Intelligence Community specifically perform our mission will probably be far greater in scope and impact than ever. Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems. These developments will pose challenges to our cyber defenses and operational tradecraft but also create new opportunities for our own intelligence collectors.

Internet of Things (IoT). "Smart" devices incorporated into the electric grid, vehicles—including autonomous vehicles—and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services. In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

Artificial Intelligence (AI). AI ranges from "Narrow AI" systems, which seek to execute specialized tasks, such as speech recognition, to "General AI" systems—perhaps still decades away—which aim to replicate many aspects of human cognition. Implications of broader AI deployment include increased vulnerability to cyberattack, difficulty in ascertaining attribution, facilitation of advances in foreign weapon and intelligence systems, the risk of accidents and related liability issues, and unemployment. Although the United States leads AI research globally, foreign state research in AI is growing.

The increased reliance on AI for autonomous decisionmaking is creating new vulnerabilities to cyberattacks and influence operations. As we have already seen, false data and unanticipated algorithm behaviors have caused significant fluctuations in the stock market because of the reliance on automated trading of financial instruments. Efficiency and performance benefits can be derived from increased reliance on AI systems in both civilian industries and national security, as well as potential gains to cybersecurity from automated computer network defense. However, AI systems are susceptible to a range of disruptive and deceptive tactics that might be difficult to anticipate or quickly understand. Efforts to mislead or compromise automated systems might create or enable further opportunities to disrupt or damage critical infrastructure or national security networks.

Foreign Data Science. This field is becoming increasingly mature. Foreign countries are openly purchasing access to published US research through aggregated publication indices, and they are collecting social media and patent data to develop their own indices.

Augmented Reality (AR) and Virtual Reality (VR). AR and VR systems with three-dimensional imagery and audio, user-friendly software, and low price points are already on the market; their adoption will probably accelerate in 2016. AR provides users with additional communications scenarios (e.g. by using virtual avatars) as well as acquisition of new data (e.g. from facial recognition) overlaid onto reality. VR gives users experiences in man-made environments wholly separate from reality.

Protecting Information Resources

Integrity. Future cyber operations will almost certainly include an increased emphasis on changing or manipulating data to compromise its integrity (i.e., accuracy and reliability) to affect decisionmaking, reduce trust in systems, or cause adverse physical effects. Broader adoption of IoT devices and AI—in settings such as public utilities and health care—will only exacerbate these potential effects. Russian cyber actors, who post disinformation on commercial websites, might seek to alter online media as a means to influence public discourse and create confusion. Chinese military doctrine outlines the use of cyber deception operations to conceal intentions, modify stored data, transmit false data, manipulate the flow of information, or influence public sentiments—all to induce errors and miscalculation in decisionmaking.

Infrastructure. Countries are becoming increasingly aware of both their own weaknesses and the asymmetric offensive opportunities presented by systemic and persistent vulnerabilities in key infrastructure sectors including health care, energy, finance, telecommunications, transportation, and water. For example, the US health care sector is rapidly evolving in ways never before imagined, and the cross-networking of personal data devices, electronic health records, medical devices, and hospital networks might play unanticipated roles in patient outcomes. Such risks are only heightened by large-scale theft of health care data and the internationalization of critical US supply chains and service infrastructure.

A major US network equipment manufacturer acknowledged last December that someone repeatedly gained access to its network to change source code in order to make its products' default encryption breakable. The intruders also introduced a default password to enable undetected access to some target networks worldwide.

Interoperability. Most governments are exploring ways to exert sovereign control over information accessible to and used by their citizens and are placing additional legal requirements on companies as they seek to balance security, privacy, and economic concerns. We assess that many countries will implement new laws and technologies to censor information, decrease online anonymity, and localize data within their national borders. Although these regulations will restrict freedoms online and increase the operating costs for US companies abroad, they will probably not introduce obstacles that threaten the functionality of the Internet.

Identity. Advances in the capabilities of many countries to exploit large data sets almost certainly increase the intelligence value of collecting bulk data and have probably contributed to increased targeting of personally identifiable information. Commercial vendors, who aggregate the bulk of digitized information about persons, will increasingly collect, analyze, and sell it to both foreign and domestic customers. We assess that countries are exploiting personal data to inform a variety of counterintelligence operations.

Accountability. Information security professionals will continue to make progress in attributing cyber operations and tying events to previously identified infrastructure or tools that might enable rapid attribution in some cases. However, improving offensive tradecraft, the use of proxies, and the creation of cover organizations will hinder timely, high-confidence attribution of responsibility for state-sponsored cyber operations.

Restraint. Many actors remain undeterred from conducting reconnaissance, espionage, and even attacks in cyberspace because of the relatively low costs of entry, the perceived payoff, and the lack of significant consequences. Moscow and Beijing, among others, view offensive cyber capabilities as an important geostrategic tool and will almost certainly continue developing them while simultaneously discussing normative frameworks to restrict such use. Diplomatic efforts in the past three years have created the foundation for establishing limits on cyber operations, and the norms articulated in a 2015 report of the UN Group of Governmental Experts suggest that countries are more likely to commit to limitations on what cyber operations can target than to support bans on the development of offensive capabilities or on specific means of cyber intervention. For example, in 2015, following a US-Chinese bilateral agreement, G-20 leaders agreed that that no country should conduct or sponsor cyber espionage for the purpose of commercial gain.

Leading Threat Actors

Russia. Russia is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations even when detected and under increased public scrutiny. Russian cyber operations are likely to target US interests to support several strategic objectives: intelligence gathering to support Russian decisionmaking in the Ukraine and Syrian crises, influence operations to support military and political objectives, and continuing preparation of the cyber environment for future contingencies.

China. China continues to have success in cyber espionage against the US Government, our allies, and US companies. Beijing also selectively uses cyberattacks against targets it believes threaten Chinese domestic stability or regime legitimacy. We will monitor compliance with China's September 2015 commitment to refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property with the intent of providing competitive advantage to companies or commercial sectors. Private-sector security experts have identified limited ongoing cyber activity from China but have not verified state sponsorship or the use of exfiltrated data for commercial gain.

Iran. Iran used cyber espionage, propaganda, and attacks in 2015 to support its security priorities, influence events, and counter threats—including against US allies in the region.

North Korea. North Korea probably remains capable and willing to launch disruptive or destructive cyberattacks to support its political objectives. South Korean officials have concluded that North Korea was probably responsible for the compromise and disclosure of data from a South Korean nuclear plant.

Nonstate Actors. Terrorists continue to use the Internet to organize, recruit, spread propaganda, collect intelligence, raise funds, and coordinate operations. In a new tactic, ISIL actors targeted and released sensitive information about US military personnel in 2015 in an effort to spur "lone-wolf" attacks. Criminals develop and use sophisticated cyber tools for a variety of purposes such as theft, extortion, and

facilitation of other criminal activities such as drug trafficking. "Ransomware" designed to block user access to their own data, sometimes by encrypting it, is becoming a particularly effective and popular tool for extortion for which few options for recovery are available. Criminal tools and malware are increasingly being discovered on state and local government networks.

TERRORISM

The United States and its allies are facing a challenging threat environment in 2016. Sunni violent extremism has been on an upward trajectory since the late 1970s and has more groups, members, and safe havens than at any other point in history. At the same time, Shia violent extremists will probably deepen sectarian tensions in response to real and perceived threats from Sunni violent extremists and to advance Iranian influence.

The Islamic State of Iraq and the Levant (ISIL) has become the preeminent terrorist threat because of its self-described caliphate in Syria and Iraq, its branches and emerging branches in other countries, and its increasing ability to direct and inspire attacks against a wide range of targets around the world. ISIL's narrative supports jihadist recruiting, attracts others to travel to Iraq and Syria, draws individuals and groups to declare allegiance to ISIL, and justifies attacks across the globe. The ISIL-directed November 2015 attacks in Paris and ISIL-Sinai's claim of responsibility for the late October downing of a Russian airliner in the Sinai underscore these dynamics.

Al-Qa'ida's affiliates have proven resilient and are positioned to make gains in 2016, despite counterterrorism pressure that has largely degraded the network's leadership in Afghanistan and Pakistan. They will continue to pose a threat to local, regional, and even possibly global interests as demonstrated by the January 2015 attack on French satirical newspaper *Charlie Hebdo* by individuals linked to al-Qa'ida in the Arabian Peninsula (AQAP). Other Sunni terrorist groups retain the ability to attract recruits and resources.

The United States will almost certainly remain at least a rhetorically important enemy for most violent extremists in part due to past and ongoing US military, political, and economic engagement overseas. Sunni violent extremists will probably continually plot against US interests overseas. A smaller number will attempt to overcome the logistical challenges associated with conducting attacks on the US homeland. The July 2015 attack against military facilities in Chattanooga and December 2015 attack in San Bernardino demonstrate the threat that homegrown violent extremists (HVEs) also pose to the homeland. In 2014, the FBI arrested approximately one dozen US-based ISIL supporters. In 2015, that number increased to approximately five dozen arrests. These individuals were arrested for a variety of reasons, predominantly for attempting to provide material support to ISIL.

US-based HVEs will probably continue to pose the most significant Sunni terrorist threat to the US homeland in 2016. The perceived success of attacks by HVEs in Europe and North America, such as those in Chattanooga and San Bernardino, might motivate others to replicate opportunistic attacks with little or no warning, diminishing our ability to detect terrorist operational planning and readiness. ISIL involvement in homeland attack activity will probably continue to involve those who draw inspiration from

the group's highly sophisticated media without direct guidance from ISIL leadership and individuals in the United States or abroad who receive direct guidance and specific direction from ISIL members or leaders.

ISIL's global appeal continues to inspire individuals in countries outside Iraq and Syria to travel to join the group. More than 36,500 foreign fighters—including at least 6,600 from Western countries—have traveled to Syria from more than100 countries since the conflict began in 2012. Foreign fighters who have trained in Iraq and Syria might potentially leverage skills and experience to plan and execute attacks in the West. Involvement of returned foreign fighters in terrorist plotting increases the effectiveness and lethality of terrorist attacks, according to academic studies. A prominent example is the November 2015 attacks in Paris in which the plotters included European foreign fighters returning from Syria.

ISIL's branches continue to build a strong global network that aims to advance the group's goals and often works to exacerbate existing sectarian tensions in their localities. Some of these branches will also plan to strike at Western targets, such as the downing of a Russian airliner in October by ISIL's self-proclaimed province in Egypt. In Libya, the group is entrenched in Surt and along the coastal areas, has varying degrees of presence across the country, and is well positioned to expand territory under its control in 2016. ISIL will seek to influence previously established groups, such as Boko Haram in Nigeria, to emphasize the group's ISIL identity and fulfill its religious obligations to the ISIL "caliphate."

Other terrorists and insurgent groups will continue to exploit weak governance, insecurity, and economic and political fragility in an effort to expand their areas of influence and provide safe havens for violent extremists, particularly in conflict zones. Sunni violent extremist groups are increasingly joining or initiating insurgencies to advance their local and transnational objectives. Many of these groups are increasingly capable of conducting effective insurgent campaigns, given their membership growth and accumulation of large financial and materiel caches. This trend increasingly blurs the lines between insurgent and terrorist groups as both aid local fighters, leverage safe havens, and pursue attacks against US and other Western interests.

No single paradigm explains how terrorists become involved in insurgencies. Some groups like ISIL in Syria and al-Qa'ida in the Islamic Maghreb (AQIM) in Mali have worked with local militants to incite insurgencies. Others, like Boko Haram, are the sole instigators and represent the primary threat to their respective homeland's security. Still others, including al-Shabaab, are the primary beneficiaries of an insurgency started by others. Finally, other groups, such as core al-Qa'ida, have taken advantage of the relative safe haven in areas controlled by insurgent groups to build capabilities and alliances without taking on a primary leadership role in the local conflict.

Although al-Qa'ida's presence in Afghanistan and Pakistan has been significantly degraded, it aspires to attack the US and its allies. In Yemen, the proven capability of AQAP to advance external plots during periods of instability suggests that leadership losses and challenges from the Iranian-backed Huthi insurgency will not deter its efforts to strike the West. Amid this conflict, AQAP has made territorial gains in Yemen including the seizure of military bases in the country's largest province. Al-Qa'ida nodes in Syria, Pakistan, Afghanistan, and Turkey are also dedicating resources to planning attacks. Al-Shabaab, al-Qaida's affiliate in East Africa, continues its violent insurgency in southern and central Somalia despite losses of territory and influence and conflict among senior leaders.

Iran—the foremost state sponsor of terrorism—continues to exert its influence in regional crises in the Middle East through the Islamic Revolutionary Guard Corps—Qods Force (IRGC-QF), its terrorist partner Lebanese Hizballah, and proxy groups. It also provides military and economic aid to its allies in the region. Iran and Hizballah remain a continuing terrorist threat to US interests and partners worldwide.

Terrorists will almost certainly continue to benefit in 2016 from a new generation of recruits proficient in information technology, social media, and online research. Some terrorists will look to use these technologies to increase the speed of their communications, the availability of their propaganda, and ability to collaborate with new partners. They will easily take advantage of widely available, free encryption technology, mobile-messaging applications, the dark web, and virtual environments to pursue their objectives.

Long-term economic, political, and social problems, as well as technological changes, will contribute to the terrorist threat worldwide. A record-setting 60 million internally displaced persons (IDPs) and refugees as of 2014—one half of whom are children, according to the United Nations—will stress the capacity of host nations already dealing with problems relating to assimilation and possibly make displaced populations targets for recruitment by violent extremists. Among Sunni violent extremist groups, ISIL is probably most proficient at harnessing social media to disseminate propaganda and solicit recruits among a broad audience. It is likely to continue these activities in 2016 by using videos, photos, and other propaganda glorifying life under ISIL rule and promoting the group's military successes. In addition, violent extremist supporters will probably continue to publicize their use of encrypted messaging applications on social media to let aspiring violent extremists know that secure avenues are available by which they can communicate.

The acute and enduring nature of demographic, economic, political, social, and technological factors contribute to the motivation of individuals and groups and their participation in violent extremist activities. These factors ensure that terrorism will remain one of several primary national security challenges for the United States in 2016.

WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

Nation-state efforts to develop or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Use of chemical weapons in Syria by both state and nonstate actors demonstrates that the threat of WMD is real. Biological and chemical materials and technologies, almost always dual use, move easily in the globalized economy, as do personnel with the scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse rapidly around the globe.

North Korea Developing WMD-Applicable Capabilities

North Korea's nuclear weapons and missile programs will continue to pose a serious threat to US interests and to the security environment in East Asia in 2016. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance to Syria's

construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

We judge that North Korea conducted a nuclear test on 6 January 2016 that it claimed was a successful test of a "hydrogen bomb." Although we are continuing to evaluate this event, the low yield of the test is not consistent with a successful test of a thermonuclear device. In 2013, following North Korea's third nuclear test, Pyongyang announced its intention to "refurbish and restart" its nuclear facilities, to include the uranium enrichment facility at Yongbyon and its graphite-moderated plutonium production reactor, which was shut down in 2007. We assess that North Korea has followed through on its announcement by expanding its Yongbyon enrichment facility and restarting the plutonium production reactor. We further assess that North Korea has been operating the reactor long enough so that it could begin to recover plutonium from the reactor's spent fuel within a matter of weeks to months.

North Korea has also expanded the size and sophistication of its ballistic missile forces—from close-range ballistic missiles to intercontinental ballistic missiles (ICBMs)—and continues to conduct test launches. In May 2015, North Korea claimed that it successfully tested a ballistic missile from a submarine. Pyongyang is also committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States; it has publicly displayed its KN08 road-mobile ICBM on multiple occasions. We assess that North Korea has already taken initial steps toward fielding this system, although the system has not been flight-tested.

Although North Korea issues official statements that include its justification for building nuclear weapons and threats to use them as a defensive or retaliatory measure, we do not know the details of Pyongyang's nuclear doctrine or employment concepts. We have long assessed that Pyongyang's nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.

China Modernizing Nuclear Forces

The Chinese People's Liberation Army's (PLA's) has established a Rocket Force—replacing the longstanding Second Artillery Corps—and continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second-strike capability. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines—armed with JL-2 SLBMs—will give the PLA Navy its first long-range, sea-based nuclear capability.

Russian Cruise Missile Violates the INF Treaty

Russia has developed a ground-launched cruise missile that the United States has declared is in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. Russia has denied it is violating the INF Treaty. In 2013, a senior Russian administration official stated publicly that the world had changed since the INF Treaty was signed 1987 and noted that Russia was "developing appropriate weapons systems" in light of the proliferation of intermediate- and shorter-range ballistic missile technologies around the world, and Russian officials have made statements in the past regarding the unfairness of a Treaty that prohibits

Russia, but not some of its neighbors, from developing and processing ground-launched missiles with ranges between 500 to 5,500 kilometers.

Chemical Weapons in Syria and Iraq

We assess that Syria has not declared all the elements of its chemical weapons program to the Chemical Weapons Convention (CWC). Despite the creation of a specialized team and months of work by the Organization for the Prohibition of Chemical Weapons (OPCW) to address gaps and inconsistencies in Syria's declaration, numerous issues remain unresolved. Moreover, we continue to judge that the Syrian regime has used chemicals as a means of warfare since accession to the CWC in 2013. The OPCW Fact-Finding Mission has concluded that chlorine had been used on Syrian opposition forces in multiple incidents in 2014 and 2015. Helicopters—which only the Syrian regime possesses—were used in several of these attacks.

We assess that nonstate actors in the region are also using chemicals as a means of warfare. The OPCW investigation into an alleged ISIL attack in Syria in August led it to conclude that at least two people were exposed to sulfur mustard. We continue to track numerous allegations of ISIL's use of chemicals in attacks in Iraq and Syria, suggesting that attacks might be widespread.

Iran Adhering to Deal To Preserve Capabilities and Gain Sanctions Relief

Iran probably views the Joint Comprehensive Plan of Action (JCPOA) as a means to remove sanctions while preserving some of its nuclear capabilities, as well as the option to eventually expand its nuclear infrastructure. We continue to assess that Iran's overarching strategic goals of enhancing its security, prestige, and regional influence have led it to pursue capabilities to meet its nuclear energy and technology goals and give it the ability to build missile-deliverable nuclear weapons, if it chooses to do so. Its pursuit of these goals will dictate its level of adherence to the JCPOA over time. We do not know whether Iran will eventually decide to build nuclear weapons.

We also continue to assess that Iran does not face any insurmountable technical barriers to producing a nuclear weapon, making Iran's political will the central issue. Iran's implementation of the JCPOA, however, has extended the amount of time Iran would need to produce fissile material for a nuclear weapon from a few months to about a year. The JCPOA has also enhanced the transparency of Iran's nuclear activities, mainly through improved access by the International Atomic Energy Agency (IAEA) and investigative authorities under the Additional Protocol to its Comprehensive Safeguard Agreement.

As a result, the international community is well postured to quickly detect changes to Iran's declared nuclear facilities designed to shorten the time Iran would need to produce fissile material. Further, the JCPOA provides tools for the IAEA to investigate possible breaches of prohibitions on specific R&D activities that could contribute to the development of a nuclear weapon.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran's ballistic missiles are inherently capable of delivering WMD, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Iran's progress on space launch vehicles—along with its desire to deter the United States and its allies—provides Tehran with the means and motivation to develop longer-range missiles, including ICBMs.

Genome Editing

Research in genome editing conducted by countries with different regulatory or ethical standards than those of Western countries probably increases the risk of the creation of potentially harmful biological agents or products. Given the broad distribution, low cost, and accelerated pace of development of this dual-use technology, its deliberate or unintentional misuse might lead to far-reaching economic and national security implications. Advances in genome editing in 2015 have compelled groups of high-profile US and European biologists to question unregulated editing of the human germline (cells that are relevant for reproduction), which might create inheritable genetic changes. Nevertheless, researchers will probably continue to encounter challenges to achieve the desired outcome of their genome modifications, in part because of the technical limitations that are inherent in available genome editing systems.

SPACE AND COUNTERSPACE

Space

Global Trends. Changes in the space sector will evolve more quickly in the next few years as innovation becomes more ubiquitous, driven primarily by increased availability of technology and growing private company investment. The number of space actors is proliferating, with 80 countries participating in space activities and more expected in the next few years. New entrants from the private space sector—leveraging lowering costs in aerospace technology and innovations in other technology sectors, such as big data analytics, social media, automation, and additive manufacturing—will increase global access to space-enabled applications, such as imaging, maritime automatic identification system (AIS), weather, Internet, and communications.

Military and Intelligence. Foreign governments will expand their use of space services—to include reconnaissance, communications, and position, navigation, and timing (PNT)—for military and intelligence purposes, beginning to rival the advantages space-enabled services provide the United States. Russia and China continue to improve the capabilities of their military and intelligence satellites and grow more sophisticated in their operations. Russian military officials publicly tout their use of imaging and electronic-reconnaissance satellites to support military operations in Syria—revealing some of their sophisticated military uses of space services.

Counterspace

Threats to our use of military, civil, and commercial space systems will increase in the next few years as Russia and China progress in developing counterspace weapon systems to deny, degrade, or disrupt US space systems. Foreign military leaders understand the unique advantages that space-based systems provide to the United States. Russia senior leadership probably views countering the US space advantage as a critical component of warfighting. Its 2014 Military Doctrine highlights at least three space-enabled capabilities—"global strike," the "intention to station weapons in space," and "strategic non-nuclear precision weapons"—as main external military threats to the Russian Federation. Russia and China are also employing more sophisticated satellite operations and are probably testing dual-use technologies in space that could be applied to counterspace missions.

Deny and Disrupt. We already face a global threat from electronic warfare systems capable of jamming satellite communications systems and global navigation space systems. We assess that this technology will continue to proliferate to new actors and that our more advanced adversaries will continue to develop more sophisticated systems in the next few years. Russian defense officials acknowledge that they have deployed radar-imagery jammers and are developing laser weapons designed to blind US intelligence and ballistic missile defense satellites.

Destroy. Russia and China continue to pursue weapons systems capable of destroying satellites on orbit, placing US satellites at greater risk in the next few years. China has probably made progress on the antisatellite missile system that it tested in July 2014. The Russian Duma officially recommended in 2013 that Russia resume research and development of an airborne antisatellite missile to "be able to intercept absolutely everything that flies from space."

COUNTERINTELLIGENCE

The United States will continue to face a complex foreign intelligence threat environment in 2016. We assess that the leading state intelligence threats to US interests will continue to be Russia and China, based on their capabilities, intent, and broad operational scope. Other states in South Asia, the Near East, East Asia, and Latin America will pose local and regional intelligence threats to US interests. For example, Iranian and Cuban intelligence and security services continue to view the United States as a primary threat.

Penetrating and influencing the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for numerous foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions involved with defense, energy, finance, dual-use technology, and other sensitive areas will remain a persistent threat to US interests.

Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016. The sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact.

Nonstate entities, including international terrorist groups and transnational organized crime organizations, will continue to employ and potentially improve their intelligence capabilities, which include human, cyber, and technical means. Like state intelligence services, these nonstate entities recruit human sources and conduct physical and technical surveillance to facilitate their activities and avoid detection and capture.

TRANSNATIONAL ORGANIZED CRIME

Some US Drug Threats Are Growing

Transnational drug trafficking poses a strong and in many cases growing threat to the United States at home and to US security interests abroad. Supplies of some foreign-produced drugs in the United States are rising, and some criminals who market them are growing more sophisticated.

- Mexican drug traffickers, capitalizing on the strong US demand for heroin, have increased heroin production significantly since 2007. US border seizures nearly doubled between 2010 and 2014. Some Mexican trafficking groups—which collectively supply most of the heroin consumed in the United States—have mastered production of the white heroin preferred in eastern US cities and have been boosting overall drug potency by adding fentanyl. Fentanyl, which is 30 to 50 times more potent than heroin, is sometimes used as an adulterant and mixed with lower-grade heroin to increase its effects or mixed with diluents and sold as "synthetic heroin" with or without the buyers' knowledge.

- Mexican traffickers have probably increased their production of the stimulant methamphetamine for the US market. US border seizures of the drug rose by nearly half between 2013 and 2014.

- Traffickers in the Andean countries have increased their manufacture of cocaine. Producers in Colombia—from which most US cocaine originates—increased output by nearly a third in 2014 over the prior year. Cocaine output will probably rise again in 2016 as previously planted coca crops fully mature.

- US availability of some new psychoactive substances—so-called "designer drugs" typically produced in Asia—has been increasing; UN scientists have identified more than 500 unique substances.

Transnational Organized Crime Groups Target Vulnerable States

Transnational organized crime groups will pose a persistent and at times sophisticated threat to the wealth, health, and security of people around the globe. Criminal groups' untaxed and unregulated enterprises drain state resources, crowd out legitimate commerce, increase official corruption, and impede economic competitiveness and fair trade. On occasion, transnational organized crime groups threaten countries' security, spur increases in social violence, or otherwise reduce governability.

- Profit-minded criminals generally do not seek the reins of political power but rather to suborn, co-opt, or bully government officials in order to create environments in which criminal enterprise can thrive.

- Foreign-based transnational criminals are increasingly using online information systems to breach sovereign borders virtually, without the need to send criminal operatives abroad to advance illicit businesses.

- Organized crime and rebel groups in Africa and elsewhere are likely to increase their involvement in wildlife trafficking to fund political activities, enhance political influence, and purchase weapons. Illicit trade in wildlife, timber, and marine resources endangers the environment, threatens good

governance and border security in fragile regions, and destabilizes communities whose economic well-being depends on wildlife for biodiversity and ecotourism. Increased demand for ivory and rhino horn in East Asia has triggered unprecedented increases in poaching in Sub-Saharan Africa.

Human trafficking exploits and abused individuals and challenges international security. Human traffickers leverage corrupt officials, porous borders, and lax enforcement to orchestrate their illicit trade. This exploitation of human lives for profit continues to occur in every country in the world—undermining the rule of law and corroding legitimate institutions of government and commerce. Trafficking in persons has become a lucrative source of revenue for transnational organized crime groups and terrorist organizations and is estimated to produce tens of billions of dollars annually. For example, terrorist or armed groups—such as ISIL, the Lord's Resistance Army, and Boko Haram—engage in kidnapping for the purpose of sexual slavery, sexual exploitation, and forced labor. These activities might also contribute to the funding and sustainment of such groups.

We assess that the ongoing global migration crises—a post-WWII record 60 million refugees and internally displaced persons—will fuel an increase in the global volume of human trafficking victims as men, women, and children undertake risky migration ventures and fall prey to sex trafficking, forced labor, debt bondage and other trafficking crimes. This continuing rise in global displacement and dangerous migration, both forced and opportunistic movements within countries and across national borders, will probably allow criminal groups and terrorist organizations to exploit vulnerable populations.

ECONOMICS AND NATURAL RESOURCES

Global economic growth will probably remain subdued, in part because of the deceleration of China's economy. During 2015, preliminary figures indicate that worldwide GDP growth slipped to 3.1 percent, down from 3.4 percent the previous year, although advanced economies as a group enjoyed their strongest GDP growth since 2010 at nearly 2 percent. However, developing economies, which were already dealing with broad and sharp commodity-price declines that began in 2014, saw the first net capital outflows to developed countries since the late 1980s.

GDP growth for these economies was 4 percent in 2015, the lowest since 2009. The International Monetary Fund (IMF) is forecasting a slight growth upturn in 2016 but downgraded its forecast in January for both developed and developing economies. Adverse shocks such as financial instability in emerging markets, a steeper-than-expected slowdown in China's growth, or renewed uncertainty about Greece's economic situation, might prevent the predicted gradual increase in global growth.

Macroeconomic Stability

Continued solid performance by the United States and the resumption of growth for many European states, even as the region continues to wrestle with the Greek debt crisis, will probably help boost growth rates for developed economies. However, increasing signs of a sustained deceleration of Chinese economic growth—particularly in sectors that are the most raw-material intensive—contributed to a continued decline in energy and commodity prices worldwide in 2015. Emerging markets and developing countries' difficulties were compounded by the declines in foreign investment inflows and increases in

resident capital outflows. The prospect of higher growth and interest rates in the United States is spurring net capital outflows from these countries, estimated to be more than $700 billion in 2015, compared to an average yearly inflow of more than $400 billion from 2009 to 2014. The global slowdown in trade is also contributing to a more difficult economic environment for many developing economies and might worsen if efforts to advance trade liberalization through the World Trade Organization (WTO) and regional trade deals stall.

Energy and Commodities

Weak energy and commodity prices have been particularly hard on key exporters in Latin America; Argentina and Brazil experienced negative growth and their weakened currencies contributed to domestic inflation. A steeply declining economy in Venezuela—the result of the oil-price decline and years of poor economic policy and profligate government spending—will leave Caracas struggling to avoid default in 2016. Similarly, in Africa, declining oil revenues and past mismanagement have contributed to Angolan and Nigerian fiscal problems, currency strains, and deteriorating external balances. Falling prices have also forced commodity-dependent exporters, such as Ghana, Liberia, and Zambia, to make sharp budget cuts to contain deficits. Persian Gulf oil exporters, which generally have more substantial financial reserves, have nonetheless seen a sharp increase in budget deficits.

Declining energy prices and substantial increases in North American production have also discouraged initiatives to develop new resources and expand existing projects—including in Brazil, Canada, Iraq, and Saudi Arabia. They typically take years to complete, potentially setting the stage for shortfalls in coming years when demand recovers.

Arctic

Diminishing sea ice is creating increased economic opportunities in the region and simultaneously raising Arctic nations' concerns about safety and the environment. Harsh weather and longer-term economic stakes have encouraged cooperation among the countries bordering the Arctic. As polar ice recedes and resource extraction technology improves, however, economic and security concerns will raise the risk of increased competition between Arctic and non-Arctic nations over access to sea routes and resources. Sustained low oil prices would reduce the attractiveness of potential Arctic energy resources. Russia will almost certainly continue to bolster its military presence along its northern coastline to improve its perimeter defense and control over its exclusive economic zone (EEZ). It will also almost certainly continue to seek international support for its extended continental shelf claim and its right to manage ship traffic within its EEZ. Moscow might become more willing to disavow established international processes or organizations concerning Arctic governance and act unilaterally to protect these interests if Russian-Western relations deteriorate further.

HUMAN SECURITY

Environmental Risks and Climate Change

Extreme weather, climate change, environmental degradation, related rising demand for food and water, poor policy responses, and inadequate critical infrastructure will probably exacerbate—and potentially

spark—political instability, adverse health conditions, and humanitarian crises in 2016. Several of these developments, especially those in the Middle East, suggest that environmental degradation might become a more common source for interstate tensions. We assess that almost all of the 194 countries that adopted the global climate agreement at the UN climate conference in Paris in December 2015 view it as an ambitious and long-lasting framework.

- The UN World Meteorological Organization (WMO) report attributes extreme weather events in the tropics and sub-tropical zones in 2015 to both climate change and an exceptionally strong El Niño that will probably persist through spring 2016. An increase in extreme weather events is likely to occur throughout this period, based on WMO reporting. Human activities, such as the generation of greenhouse gas emissions and land use, have contributed to extreme weather events including more frequent and severe tropical cyclones, heavy rainfall, droughts, and heat waves, according to a November 2015 academic report with contributions from scientists at the National Oceanic and Atmospheric Administration (NOAA). Scientists have more robust evidence to identify the influence of human activity on temperature extremes than on precipitation extremes.

- The Paris climate change agreement establishes a political expectation for the first time that all countries will address climate change. The response to the deal has been largely positive among government officials and nongovernmental groups, probably because the agreement acknowledges the need for universal action to combat climate change along with the development needs of lower-income countries. However, an independent team of climate analysts and the Executive Secretary of the UN climate forum have stated that countries' existing national plans to address climate change will only limit temperature rise to 2.7 degrees Celsius by 2100.

Health

Infectious diseases and vulnerabilities in the global supply chain for medical countermeasures will continue to pose a danger to US national security in 2016. Land-use changes will increase animal-to-human interactions and globalization will raise the potential for rapid cross-regional spread of disease, while the international community remains ill prepared to collectively coordinate and respond to disease threats. Influenza viruses, coronaviruses such as the one causing Middle Eastern Respiratory Syndrome (MERS), and hemorrhagic fever viruses such as Ebola are examples of infectious disease agents that are passed from animals to humans and can quickly pose regional or global threats. Zika virus, an emerging infectious disease threat first detected in the Western Hemisphere in 2014, is projected to cause up to 4 million cases in 2016; it will probably spread to virtually every country in the hemisphere. Although the virus is predominantly a mild illness, and no vaccine or treatment is available, the Zika virus might be linked to devastating birth defects in children whose mothers were infected during pregnancy. Many developed and developing nations remain unable to implement coordinated plans of action to prevent infectious disease outbreaks, strengthen global disease surveillance and response, rapidly share information, develop diagnostic tools and countermeasures, or maintain the safe transit of personnel and materials.

- Human encroachment into animal habitats, including clearing land for farm use and urbanization, is recognized as a contributing factor in the emergence of new infectious diseases. The populations of Asia and Africa are urbanizing and growing faster than those of any other region, according to the

UN. Emerging diseases against which humans have no preexisting immunity or effective therapies pose significant risks of becoming pandemics.

Atrocities and Instability

Risks of atrocities, large-scale violence, and regime-threatening instability will remain elevated in 2016. A vicious cycle of conflict resulting from weak governance, the rise of violent non-state actors, insufficient international capacity to respond to these complex challenges, and an increase in global migration all contribute to global security risks. Weak global growth, particularly resulting from the cascading effect of slower Chinese growth that will hurt commodity exporters, will also exacerbate risk.

- Regional spillover will probably spread. For example, the long-term impact of civil war in Syria is reinforcing sectarian differences in Iraq, and the flight of Syrians to Turkey, Jordan, and Lebanon, and then onward to Europe is sowing regional tensions and straining national governments.

- As of 2015, the central governments of seven states are unable to project authority and provide goods and services throughout at least 50 percent of their respective territory; this number is the largest at any point in the past 60 years.

- The risk of waning support for universal human rights norms is increasing as authoritarian regimes push back against human rights in practice and in principle.

Global Displacement

Europe will almost certainly continue to face record levels of arriving refugees and other migrants in 2016 unless the drivers causing this historic movement toward the continent change significantly in 2016, which we judge is unlikely. Migration and displacement will also probably be an issue within Asia and Africa as well as the Americas. In total, about 60 million people are displaced worldwide, according to the UN High Commissioner for Refugees (UNHCR). These 60 million consist of approximately 20 million refugees, 38 million internally displaced persons (IDPs), and approximately 2 million stateless persons, also according to UNHCR statistics.

- Wars, weak border controls, and relatively easy and affordable access to routes and information are driving this historic increase in mobility and displacement.

The growing scope and scale of human displacement will probably continue to strain the response capacity of the international community and drive a record level of humanitarian requests. At the same time, host and transit countries will struggle to develop effective responses and, in some cases, manage domestic fears of terrorists exploiting migrant flows after the Paris attacks in November 2015.

- In 2015, the UN received less than half of its requested funding for global assistance, suggesting that the UN's 2016 request is also likely to be underfunded.

REGIONAL THREATS

Emerging trends suggest that geopolitical competition among the major powers is increasing in ways that challenge international norms and institutions. Russia, in particular, but also China seek greater influence over their respective neighboring regions and want the United States to refrain from actions they perceive as interfering with their interests—which will perpetuate the ongoing geopolitical and security competition around the peripheries of Russia and China, to include the major sea lanes. They will almost certainly eschew direct military conflict with the United States in favor of contests at lower levels of competition—to include the use of diplomatic and economic coercion, propaganda, cyber intrusions, proxies, and other indirect applications of military power—that intentionally blur the distinction between peace and wartime operations.

Although major power competition is increasing, the geopolitical environment continues to offer opportunities for US cooperation. In addition, despite the prospect for increased competition, the major powers, including Russia and China, will have incentives to continue to cooperate with the United States on issues of shared interest that cannot be solved unilaterally. A future international environment defined by a mix of competition and cooperation among major powers, however, will probably encourage ad-hoc approaches to global challenges that undermine existing international institutions.

EAST ASIA

China

China will continue to pursue an active foreign policy—especially within the Asia Pacific—highlighted by a firm stance on competing territorial claims in the East and South China Seas, relations with Taiwan, and its pursuit of economic engagement across East Asia. Regional tension will continue as China pursues construction at its expanded outposts in the South China Sea and because competing claimants might pursue actions that others perceive as infringing on their sovereignty. Despite the meeting between China's and Taiwan's Presidents in November 2015, Chinese leaders will deal with a new president from a different party in Taiwan following elections in January. China will also pursue efforts aimed at fulfilling its "One Belt, One Road" initiative to expand China's economic role and outreach across Asia.

China will continue to incrementally increase its global presence. Mileposts have included symbolic and substantive developments, such as the IMF's decision in November 2016 to incorporate the renminbi into its Special Drawing Rights currency basket and China's opening of the Asian Infrastructure Investment Bank in early 2016. China will increasingly be a factor in global responses to emerging problems, as illustrated by China's participation in UN peacekeeping operations, WHO's Ebola response, and infrastructure construction in Africa and Pakistan.

Amid new economic challenges, Chinese leaders are pursuing an ambitious agenda of economic, legal, and military reforms aimed at bolstering the country's long-term economic growth potential, improving

government efficiency and accountability, and strengthening the control of the Communist Party. The scope and scale of the reform agenda—coupled with an ongoing anti-corruption campaign—might increase the potential for internal friction within China's ruling Communist Party. Additionally, China's leaders, who have declared slower economic growth to be the "new normal," will nonetheless face pressure to stabilize growth at levels that still support strong job creation.

Southeast Asia

Regional integration via the Association of Southeast Asian Nations (ASEAN) made gains in 2015 with the establishment of the ASEAN Community. However, ASEAN cohesion on economic and security issues will continue to face challenges stemming from differing development levels among ASEAN members and their varying threat perceptions of China's regional ambitions and assertiveness in the South China Sea.

Democracy in many Southeast Asian nations remains fragile. Elites—rather than the populace—retain a significant level of control and often shape governance reforms to benefit their individual interests rather than to promote democratic values. Corruption and cronyism continue to be rampant in the region, and the rising threat of ISIL might provide some governments with a new rationale to not only address the terrorist threat but also curb opposition movements, like some leaders in the region did in the post 9/11 environment. The new National League for Democracy-led government in Burma is poised to continue the country's democratic transition process, but given its lack of governing experience, the learning curve will be steep. The Burmese constitution also ensures that the military will retain a significant level of power in the government, hampering the NLD to put its own stamp on the ongoing peace process. In Thailand, the military-led regime is positioned to remain in power through 2017.

North Korea

Since taking the helm of North Korea in December 2011, Kim Jong Un has further solidified his position as the unitary leader and final decision authority through purges, executions, and leadership shuffles. Kim and the regime have publicly emphasized—and codified—North Korea's focus on advancing its nuclear weapons program, developing the country's troubled economy, and improving the livelihood of the North Korean people, while maintaining the tenets of a command economy. Despite efforts at diplomatic outreach, Kim continues to challenge the international community with provocative and threatening behavior in pursuit of his goals, as prominently demonstrated in the November 2014 cyberattack on Sony, the August 2015 inter-Korean confrontation spurred by the North's placement of landmines that injured two South Korean soldiers, and the fourth nuclear test in January 2016.

RUSSIA AND EURASIA

Russia

Moscow's more assertive foreign policy approach, evident in Ukraine and Syria, will have far-reaching effects on Russia's domestic politics, economic development, and military modernization efforts.

President Vladimir Putin has sustained his popular approval at or near record highs for nearly two years after illegally annexing Crimea. Nevertheless, the Kremlin's fears of mass demonstration remain high, and the government will continue to rely on repressive tactics to defuse what it sees as potential catalysts for protests in Russia. The Kremlin's fear of instability and its efforts to contain it will probably be especially acute before the September 2016 Duma election.

The Russian economy will continue to shrink as a result of longstanding structural problems—made worse by low energy prices and economic sanctions—and entered into recession in 2015. A consensus forecast projects that GDP will contract by 3.8 percent in 2015 and will probably decline between 2-3 percent in 2016 if oil prices remain around $40 per barrel or only 0.6 percent if oil returns to $50 per barrel. Real wages declined throughout most of 2015 and the poverty rate and inflation have also worsened.

We assess that Putin will continue to try to use the Syrian conflict and calls for cooperation against ISIL to promote Russia's Great Power status and end its international isolation. Moscow's growing concern about ISIL and other extremists has led to direct intervention on the side of Bashar al-Asad's regime and efforts to achieve a political resolution to the Syrian conflict on Russia's terms. Since the terrorist attacks in Paris and over the Sinai, Russia has redoubled its calls for a broader anti-terrorism coalition. Meanwhile, growing Turkish-Russian tensions since Turkey's shootdown of a Russian jet in November 2015 raise the specter of miscalculation and escalation.

Despite Russia's economic slowdown, the Kremlin remains intent on pursuing an assertive foreign policy in 2016. Russia's willingness to covertly use military and paramilitary forces in a neighboring state continues to cause anxieties in states along Russia's periphery, to include NATO allies. Levels of violence in eastern Ukraine have decreased, but Moscow's objectives in Ukraine—maintaining long-term influence over Kyiv and frustrating Ukraine's attempts to integrate into Western institutions—will probably remain unchanged in 2016.

Since the crisis began in Ukraine in 2014, Moscow has redoubled its efforts to reinforce its influence in Eurasia. Events in Ukraine raised Moscow's perceived stakes for increasing its presence in the region to prevent future regime change in the former Soviet republics and for accelerating a shift to a mulitpolar world in which Russia is the uncontested regional hegemon in Eurasia. Moscow will therefore continue to push for greater regional integration, raising pressure on neighboring states to follow the example of Armenia, Belarus, Kazakhstan, and Kyrgyzstan and join the Moscow-led Eurasian Economic Union.

Moscow's military foray into Syria marks its first use of significant expeditionary combat power outside the post-Soviet space in decades. Its intervention underscores both the ongoing and substantial improvements in Russian military capabilities and the Kremlin's confidence in using them as a tool to advance foreign policy goals. Despite its economic difficulties, Moscow remains committed to modernizing its military.

Russia continues to take information warfare to a new level, working to fan anti-US and anti-Western sentiment both within Russia and globally. Moscow will continue to publish false and misleading information in an effort to discredit the West, confuse or distort events that threaten Russia's image, undercut consensus on Russia, and defend Russia's role as a responsible and indispensable global power.

Ukraine, Belarus, and Moldova

The implementation timeline for the Minsk agreements has been extended through 2016, although opposition from **Ukraine**, Russia, and the separatists on key remaining Minsk obligations might make progress slow and difficult in 2016. Sustained violence along the Line of Contact delineating the separatist-held areas will probably continue to complicate a political settlement, and the potential for escalation remains.

Ukraine has made progress in its reform efforts and its moves to bolster ties to Western institutions. Ukraine will continue to face serious challenges, however, including sustaining progress on key reforms and passing constitutional amendments—required under the Minsk agreements to devolve political power and fiscal authority to the regions.

Belarus continues its geopolitical balancing act, attempting to curry favor with the West without antagonizing Russia. President Lukashenko released several high-profile political prisoners in August 2015 and secured reelection to a fifth term in October 2015 without cracking down on the opposition as he has in previous elections. These developments prompted the EU and the United States to implement temporary sanctions relief, providing a boost to a Belarusian economy.

Moldova faces a turbulent year in 2016. Popular discontent over government corruption and misrule continues to reverberate after a banking scandal sparked large public protests, and political infighting brought down a government coalition of pro-European parties in October 2015. Continued unrest is likely. The breakaway pro-Russian region is also struggling economically and will remain dependent on Russian support.

The Caucasus and Central Asia

Even as **Georgia** progresses with reforms, Georgian politics will almost certainly be volatile as political competition increases. Economic challenges are also likely to become a key political vulnerability for the government before the 2016 elections. Rising frustration among Georgia's elites and the public with the slow pace of Western integration and increasingly effective Russian propaganda raise the prospect that Tbilisi might slow or suspend efforts toward greater Euro-Atlantic integration. Tensions with Russia will remain high, and we assess that Moscow will raise the pressure on Tbilisi to abandon closer EU and NATO ties.

Tensions between **Armenia** and **Azerbaijan** over the separatist region of Nagorno-Karabakh remained high in 2015. Baku's sustained military buildup coupled with declining economic conditions in Azerbaijan are raising the potential that the conflict will escalate in 2016. Azerbaijan's aversion to publicly relinquishing its claim to Nagorno-Karabakh proper and Armenia's reluctance to give up territory it controls will continue to complicate a peaceful resolution.

Central Asian states remain concerned about the rising threat of extremism to the stability of their countries, particularly in light of a reduced Coalition presence in Afghanistan. Russia shares these concerns and is likely to use the threat of instability in Afghanistan to increase its involvement in Central Asian security affairs. However, economic challenges stemming from official mismanagement, low commodity prices, declining trade and remittances associated with Russia's weakening economy, and

ethnic tensions and political repression, are likely to present the most significant instability threat to these countries.

EUROPE

Key Partners

European governments will face continued political, economic, and security challenges deriving from mass migration to Europe, terrorist threats, a more assertive Russia, and slow economic recovery. Differences among national leaders over how best to confront the challenges are eroding support for deeper EU integration and will bolster backing for populist leaders who favor national prerogatives over EU-wide remedial strategies.

The European Commission expects 1.5 million migrants to arrive in Europe in 2016—an influx that is prompting European officials to focus on improving border security, particularly at the Schengen Zone's external borders, and putting the free movement of people within the EU at risk. Several European governments are using military forces in domestic security roles.

The European Commission has warned against drawing a link between terrorists and refugees, but populist and far-right leaders throughout Europe are preying on voters' security fears by highlighting the potential dangers of accepting migrants fleeing war and poverty. Some EU leaders are citing the November 2015 terrorist attacks in Paris to justify erecting fences to stem the flow of people.

European countries will remain active and steadfast allies on the range of national security threats that face both the United States and Europe—from energy and climate change to countering violent extremism and promoting democracy. Although the majority of NATO allies have successfully halted further declines in defense spending, European military modernization efforts will take several years before marked improvement begins to show.

Europe also continues to insist on full implementation of the Minsk agreement to stop violence in Ukraine. However, European governments differ on the proper extent of engagement with Moscow.

Europe's economic growth, which the EU projects will be moderate, could falter if emerging market economies slow further, which would decrease the demand for European exports. The EU continues to struggle to shake off the extended effects of its economic recession, with lingering worries over high unemployment, weak demand, and lagging productivity. Greece also remains a concern for the EU. The agreement between Greece and its creditors is an important step forward for restoring trust among the parties and creating the conditions for a path forward for Greece within the Eurozone. Developing the details of the agreement and its full implementation remain challenges.

The Balkans

Ethnic nationalism and weak institutions in the Balkans remain enduring threats to stability. Twenty years after the end of the Bosnian War and the signing of the Dayton Agreement, Bosnia and Herzegovina

remains culturally and administratively divided, weighed down by a barely functional and inefficient bureaucracy. The country, one of Europe's poorest, has endured negative GDP growth since the 2008 international financial crisis and is reliant on the support of international institutions including the IMF. Youth unemployment, estimated at 60 percent, is the world's highest.

Kosovo has made progress toward full, multiethnic democracy, although tensions between Kosovo Albanians and Kosovo Serbs remain. In Macedonia, an ongoing political crisis and concerns about radicalization among ethnic Albanian Muslims threatens to aggravate already-tense relations between ethnic majority Macedonians and the country's minority Albanians, fifteen years after a violent interethnic conflict between the two groups ended. Social tensions in the region might also be exacerbated if the Western Balkans becomes an unwilling host to significant migrant populations.

Turkey

Turkey remains a partner in countering ISIL and minimizing foreign fighter flows. Ankara will continue to see the Kurdistan Workers' Party (PKK) as its number one security threat and will maintain military and political pressure on the PKK, as well as on the Democratic Union Party (PYD) and its armed affiliate People's Protection Units (YPG), which Turkey equates with the PKK. Turkey is extremely concerned about the increasing influence of the PYD and the YPG along its borders, seeing them as a threat to its territorial security and its efforts to control Kurdish separatism within its borders.

Turkey is concerned about Russia's involvement in the region in support of Asad, the removal of whom Turkey sees as essential to any peace settlement. Turkey is also wary of increased Russian cooperation with the Kurds and greater Russian influence in the region that could counter Turkey's leadership role. The Russian-Iranian partnership and Iran's attempts to expand Shiite influence in the region are also security concerns for Turkey.

The refugee flow puts significant strain on Turkey's economy, which has amounted to $9 billion according to a statement by Turkish President Recep Tayyip Erdogan. Refugees have also created infrastructure and social strains, particularly regarding access to education and employment. Turkey tightened its borders in 2015 and is working to stanch the flow of migrants to Europe and address refugee needs.

MIDDLE EAST AND NORTH AFRICA

Iraq

In Iraq, anti-ISIL forces will probably make incremental battlefield gains through spring 2016. Shia militias and Kurdish forces in northern Iraq have recaptured Bayji and Sinjar, respectively, from the Islamic State of Iraq and the Levant (ISIL). In western Iraq, the Iraqi Security Forces (ISF) have retaken most of the greater Ramadi area from ISIL and will probably clear ISIL fighters from the city's urban core in the coming month.

ISIL's governance of areas it controls is probably faltering as airstrikes take a toll on the group's sources of income, hurting ISIL's ability to provide services, and causing economic opportunities for the population

to dwindle. Even so, the Iraqi Sunni population remains fearful of the Shia-dominated government in Baghdad. This fear has been heightened as Iranian-backed Shia militias play a lead role in retaking Sunni-majority areas, suggesting Iraq's Sunnis will remain willing to endure some deprivation under ISIL rule.

Prime Minister Haydar al-Abadi will probably continue to struggle to advance his reforms—which aim to combat corruption and streamline government—because of resistance from Iraqi elites who view the reforms as threatening to their entrenched political interests. Meanwhile, the drop in oil prices is placing strain on both Baghdad's and Irbil's budgets, constraining their ability to finance counter-ISIL operations and limiting options to address potential economically driven unrest.

Syria

We assess that foreign support will allow Damascus to make gains in some key areas against the opposition and avoid further losses, but it will be unable to fundamentally alter the battlespace. Increased Russian involvement, particularly airstrikes, will probably help the regime regain key terrain in high priority areas in western Syria, such as Aleppo and near the coast, where it suffered losses to the opposition in summer 2015. ISIL is under threat on several fronts in Syria and Iraq from increased Coalition and government operations.

Manpower shortages will continue to undermine the Syrian regime's ability to accomplish strategic battlefield objectives. The regime still lacks the personnel needed to capture and hold key areas and strategically defeat the opposition or ISIL. Damascus increasingly relies on militias, reservists, and foreign supporters—such as Iran and Lebanese Hizballah--to generate manpower, according to press reporting.

The Syrian regime and most of the opposition are participating in UN-mediated talks that started in early February in Geneva. Both sides probably have low expectations for the negotiations, with the opposition calling for ceasefires and humanitarian assistance as a precondition. The negotiations, without a ceasefire agreement, will not alter the battlefield situation.

The humanitarian situation in Syria continues to deteriorate. In December 2015 and January 2016, the number of Syrian refugees registered or in the process of registering in the Middle East and North Africa rose by nearly 102,000 from 4.3 million to 4.4 million, according to UN data. The refugees are putting significant strain on countries surrounding Syria as well as on Europe. Turkey hosts more than 2.2 million refugees; Lebanon has about 1.1 million; Jordan has more than 630,000; Iraq has 245,000. Approximately 500,000 have fled to Europe, according to the UN. The more than 4 million refugees and 6.5 million estimated internally displaced persons (IDPs) account for 49 percent of Syria's preconflict population.

- Estimates of fatalities in Syria since the start of the civil war vary, but most observers calculate that at least 250,000 men, women, and children on all sides of the conflict have lost their lives since 2011.

- On 22 December, the UN Security Council unanimously adopted resolution 2258, which renews the UN's authority to utilize cross-border deliveries for humanitarian assistance to Syria through 10

January 2017. Since July 2014, the UN has provided food to 2.4 million people, water and sanitation to 1.3 million people, and medical supplies to 4.1 million people through its cross-border deliveries.

- Separately, the Syrian Government began requiring in mid-November that aid agencies get humanitarian assistance notarized by the Syrian embassies in the country of product origin. This requirement previously applied only to commercial goods and might delay future UN food deliveries within Syria, according to the UN.

Libya

We assess that insecurity and conflict in Libya will persist in 2016, posing a continuing threat to regional stability. The country has been locked in civil war between two rival governments and affiliated armed groups. The 17 December signing of a UN-brokered agreement to form a Government of National Accord (GNA) resulted from a year-long political dialogue that sought to end the ongoing civil war and reconcile Libya's rival governments. However, the GNA will face a number of obstacles in establishing its authority and security across the country. The GNA still faces the difficult task of forming a capable, centralized security force. It will also be challenged to confront terrorist groups such as ISIL, which has exploited the conflict and political instability in the country to expand its presence.

- The rival governments—the internationally recognized Tobruk-based House of Representatives (House) and the Tripoli-based General National Congress (GNC) have participated in UN-brokered peace talks since fall 2014. Reaction to the deal and the proposed GNA has been mixed, and hardliners on both sides have opposed the agreement.

- (U) On 25 January, the House voted to approve the UN-brokered deal with conditions but rejected a controversial article granting the GNA's Presidency Council interim control of the military. The House also rejected the GNA's proposed cabinet and demanded a smaller ministerial slate.

- Libya's economy has deteriorated because of the conflict. Oil exports—the primary source of government revenue—have fallen significantly from the pre-revolution level of 1.6 billion barrels per day. Libya's oil sector also faces continued threats from terrorist groups; ISIL attacked oil production and export facilities in February 2015, September 2015, and January 2016.

Meanwhile, extremists and terrorists have exploited the security vacuum to plan and launch attacks in Libya and throughout the region. The permissive security environment has enabled ISIL to establish one of its most developed branches outside of Syria and Iraq. As of late 2015, ISIL's branch in Libya maintained a presence in Surt, Benghazi, Tripoli, Ajdabiya, and other areas of the country, according to press reports. Members of ISIL in Libya continue to stage attacks throughout the country.

Yemen

The Yemen conflict will probably remain in a strategic stalemate through mid-2016. Negotiations between the Saudi-led coalition and the Huthi-aligned forces remain stalled, but neither side is able to achieve decisive results through military force. Huthi-aligned forces almost certainly remain committed to fighting following battlefield setbacks in the Aden and Marib Governorates in 2015 and probably intend to retake lost territory in those areas.

Nonetheless, regional stakeholders on both sides of Yemen's conflict, including Iran, which continues to back the Huthis, are signaling willingness to participate in peace talks. Even a cease-fire of a few days or weeks would facilitate the entry and distribution of commercial and humanitarian goods inside Yemen, where at least 21 million people—80 percent of the population—require assistance, according to the UN.

AQAP and ISIL's affiliates in Yemen have exploited the conflict and the collapse of government authority to gain new recruits and allies and expand their territorial control. In December, AQAP seized the southern city of Zinjibar, adding to its capture of the coastal city of Mukalla to the east.

Iran

Since January, Tehran met the demands for implementation of the Joint Comprehensive Plan of Action (JCPOA), exchanged detainees, and released 10 US sailors. Despite these developments, the Islamic Republic of Iran presents an enduring threat to US national interests because of its support to regional terrorist and militant groups and the Asad regime, as well as its development of advanced military capabilities. Tehran views itself as leading the "axis of resistance"—which includes the Asad regime and subnational groups aligned with Iran, especially Lebanese Hizballah and Iraqi Shia militants. Their intent is to thwart US, Saudi, and Israeli influence, bolster its allies, and fight ISIL's expansion. Tehran might even use American citizens detained when entering Iranian territories as bargaining pieces to achieve financial or political concessions in line with their strategic intentions.

Iran's involvement in the Syrian, Iraqi, and Yemeni conflicts deepened in 2015. In Syria, Iran more openly acknowledged the deaths of Iranian "martyrs," increased Iranian troop levels, and took more of a frontline role against "terrorists." In Iraq, Iranian combat forces employed rockets, artillery, and drones against ISIL. Iran also supported Huthi rebels in Yemen by attempting to ship lethal aid to the Huthis. Tehran will almost certainly remain active throughout the Persian Gulf and broader Middle East in 2016 to support its regional partners and extend its regional influence. Iranian officials believe that engaging adversaries away from its borders will help prevent instability from spilling into Iran and reduce ISIL's threat to Iran and its regional partners. Iran has also increased cooperation with Russia in the region.

Supreme Leader Khamenei continues to view the United States as a major threat to Iran, and we assess that his views will not change, despite implementation of the JCPOA deal. In October 2015, Khamenei publicly claimed the United States was using the JCPOA to "infiltrate and penetrate" Iran. His statement prompted the Iranian hardliner-dominated security services to crack down on journalists and businessmen with suspected ties to the West. The crackdown was intended by hardliners to demonstrate to President Ruhani and to Washington that a broader opening to the West following JCPOA would not be tolerated. Iran released several US citizens in January 2016 who were being held in Iran; however, it might attempt to use any additional US citizens as bargaining chips for US concessions.

Iran's military and security services are keen to demonstrate that their regional power ambitions have not been altered by the JCPOA deal. One week prior to JCPOA Adoption Day, Iran publicized the launch of its new "long-range" and more accurate ballistic missile called the "Emad." Iran also publicizes development of its domestically produced weapons systems, submarines and surface combatants, artillery, and UAVs to deter potential adversaries and strengthen its regional influence and prestige.

Iran's involvement in the Syrian and Iraqi conflicts has enabled its forces to gain valuable on-the-ground experience in counterinsurgency operations.

Lebanon

Lebanon will continue to struggle with the fallout from the civil war in neighboring Syria and faces a range of interlocking political, security, humanitarian, and economic challenges. The spillover from the Syrian conflict has had negative consequences on almost all aspects of life in Lebanon, from rising sectarianism to major strains on infrastructure and public services, further straining the country's delicate political balance.

- Lebanon's most immediate security threat is from Syrian-based extremists on its northeastern border. The Lebanese army has carried out multiple operations against Nusrah Front and ISIL to secure the border and prevent against the flow of terrorists into the country. Beirut also faces threats from Sunni extremists in the country who are retaliating against Lebanese Hizballah's military involvement in the Syrian civil war.

- The influx of about 1.1 million Sunni Syrian refugees to Lebanon has altered the country's sectarian demographics and is badly straining public services and burdening the economy. The Lebanese economy will probably remain stagnant throughout 2016, as protracted regional instability and political gridlock at home continue to erode the country's competitiveness.

Egypt

Egypt faces a persistent threat of terrorist and militant activity directed primarily at state security forces in both the Sinai Peninsula and in mainland Egypt. The security services have initiated a counterterrorism campaign to disrupt and detain Sinai-based militants; however, terrorist groups still retain the ability to conduct attacks.

- ISIL's branch in Sinai (ISIL-Sinai) has conducted dozens of lethal attacks on military and security personnel, some of which suggest sophisticated and coordinated attack planning, according to press reports.

- ISIL-Sinai claimed responsibility for the downing of a Russian aircraft in the Sinai in October 2015, which, if true, would demonstrate the expanding threat from ISIL and its regional branches.

- The continued threat of terrorism places further strain on Egypt's economy by harming Egypt's tourism industry, a key source of revenue. The country is also grappling with high poverty and unemployment rates.

Tunisia

Tunisia's first post-transitional democratic government since the 2011 Arab Spring revolution is marking its first year in office. Since the revolution, the country has overcome deep political divisions to reach consensus on key political issues, develop a new constitution, and elect a new government, according to

press and academic reports. Despite the government's significant strides in its democratic transition, Tunisia faces challenges in consolidating these achievements.

- Tunisia is confronting a threat from terrorist groups exploiting Libya's permissive environment to plan and launch attacks, as well as from groups operating within Tunisia's borders, according to press reports. The perpetrators of the terrorist attack on the Bardo Museum in Tunis in March 2015 and hotels in Sousse in June—both claimed by ISIL—trained at a terrorist camp in Libya, according to press reports.

- The government inherited high unemployment, particularly among youth, and a high budget deficit according to press reports. The Bardo and Sousse terrorist attacks have disrupted tourism, a critical source of revenues and jobs.

SOUTH ASIA

Afghanistan

The Kabul Government will continue to face persistent hurdles to political stability in 2016, including eroding political cohesion, assertions of authority by local powerbrokers, recurring financial shortfalls, and countrywide, sustained attacks by the Taliban. Political cohesion will remain a challenge for Kabul as the National Unity Government will confront larger and more divisive issues later in 2016, including the implementation of election reforms, long-delayed parliamentary elections, and a potential change by a Loya Jirga that might fundamentally alter Afghanistan's constitutional order. Kabul will be unable to effectively address its dire economic situation or begin to curb its dependence on foreign aid until it first contains the insurgency, which is steadily chipping away at Afghanistan's security. In this environment, international financial aid will remain the most important external determinant of the Kabul government's strength. We assess that fighting in 2016 will be more intense than 2015, continuing a decade-long trend of deteriorating security that will compound these challenges. The fighting will continue to threaten US personnel, our Allies, and international partners—including Afghans—particularly in Kabul and other urban population centers. The Afghan National Security Forces (ANSF), with the help of anti-Taliban powerbrokers and international funding, will probably maintain control of most major population centers. However, the forces will very likely cede control of some rural areas. Without international funding, the ANSF will probably not remain a cohesive or viable force.

The Taliban has largely coalesced and is relatively cohesive under the leadership of new Taliban Senior Leader Mullah Akhtar Mohammad Mansur despite some early opposition. The Taliban's two-week seizure of the provincial capital of Kunduz provided an important boost to Mansur's leadership. The Taliban will continue to test the overstretched ANSF faced with problematic logistics, low morale, and weak leadership.

The Islamic State of Iraq and the Levant (ISIL) announced in January 2015 the formation of its Khorasan branch in South Asia, an amalgamation of primarily disaffected and rebranded former Afghan Taliban and Tehrik-e Taliban Pakistan (TTP) members. Despite quick early growth in 2015, ISIL's Khorasan branch

will probably remain a low-level threat to Afghan stability as well as to US and Western interests in the region in 2016.

Bangladesh

Prime Minister Sheikh Hasina's continuing efforts to undermine the political opposition in Bangladesh will probably provide openings for transnational terrorist groups to expand their presence in the country. Hasina and other government officials have insisted publically that the killings of foreigners are the work of the Bangladesh Nationalist Party and the Bangladesh Jamaat-e Islami political parties and are intended to discredit the government. However, ISIL claimed responsibility for 11 high-profile attacks on foreigners and religious minorities. Other extremists in Bangladesh—including Ansarullah Bangla Team and al-Qa'ida in the Indian Subcontinent (AQIS)—have claimed responsibility for killing at least 11 progressive writers and bloggers in Bangladesh since 2013.

Pakistan and India

Relations between Pakistan and India remain tense despite the resumption of a bilateral dialogue in December. Following a terrorist attack in early January on Pathankot Air Force base in India, which New Delhi blames on a Pakistani-based group, India's engagement with Pakistan will probably hinge in 2016 on Islamabad's willingness to take action against those in Pakistan linked to the attack.

SUB-SAHARAN AFRICA

Central Africa

Prospects for delayed elections in the **Democratic Republic of the Congo**, originally scheduled for 2016, increase the risk of political tensions and perhaps violence. Violence might also break out in the **Republic of Congo** where a controversial October 2015 constitutional referendum paved the way for long-serving President Denis Sassou-Nguesso to run for a new term in 2016 elections. Both governments have resorted to heavy-handed tactics to stifle opposition and subdue or prevent election-related protests.

In **Burundi**, violence related to President Pierre Nkurunziza's controversial reelection in July 2015 will almost certainly continue as a simmering crisis. The conflict might expand and intensify if increased attacks between the government and armed opposition provoke a magnified response from either side or if the security services fracture into divided loyalties.

The **Central African Republic** held peaceful presidential and parliamentary elections in late December, although they were marred by logistical issues. A run-off will probably take place in mid-February between the two top candidates, and we do not know how the armed spoilers and losing candidates will react. The risk of continued ethno-religious clashes between Christians and Muslims throughout the country remains high despite the presence of international peacekeeping forces, which are increasingly targets of violence.

Somalia

The Somali Federal Government's authority will probably remain largely confined to the capital in 2016, and Mogadishu will continue to rely on the African Union Mission in Somalia (AMISOM) as a security guarantor against al-Shabaab as it prepares for elections in 2016.

South Sudan

Implementation of the peace agreement between Juba and opposition elements will be slow as spoilers from both sides seek to stall progress. The return of former opposition members to Juba will almost certainly cause jockeying for positions of power. Localized fighting will continue and probably spread to previously unaffected areas, causing the humanitarian situation to worsen Economic conditions will probably deteriorate further as inflation remains high and prices for staple goods rise, fueling dissatisfaction with the government.

Sudan

President Bashir consolidated power following his reelection in April 2015, but the regime will continue attempts at a national dialogue, which will probably not placate a divided political opposition. The regime will almost certainly confront a range of challenges, including public dissatisfaction over a weakened economy. Divisions among armed opponents will almost certainly inhibit their ability to make significant gains against Khartoum. However, elements of the opposition will continue to wage insurgencies in the Southern Kordofan and Blue Nile states and Darfur. Sudan, listed as a state sponsor of terror since 1993, cut diplomatic ties with Iran in January following an attack on the Saudi Embassy in Tehran. Since 2014, Sudan's relations with Iran have cooled as Khartoum has grown closer to Riyadh.

Nigeria

President Muhammadu Buhari and the Nigerian government will confront a wide range of challenges in 2016, many of which are deeply rooted and have no "quick fixes." His tasks include reviving a struggling economy – Africa's largest – diversifying sources of government revenue beyond oil, reining in corruption, addressing mounting state debts, reforming redundant parastatal organizations, and developing the power, agriculture, and transportation sectors. Nigeria will continue to face internal threats from Boko Haram, which pledged loyalty to the Islamic State in Iraq and the Levant (ISIL) in March 2015. Despite losing territory in 2015, Boko Haram will probably remain a threat to Nigeria throughout 2016 and will continue its terror campaign within the country and in neighboring Cameroon, Niger, and Chad.

LATIN AMERICA AND CARIBBEAN

Central America

Strong family ties to the United States—as well as gang violence, a lack of jobs, and a worsening drought in Central America's northern tier—will sustain high rates of migration to the United States in 2016. Weak institutions, divided legislatures, low levels of tax collection, and high debts will constrain efforts to

improve rule of law, tackle corruption, and alleviate poverty. Homicide rates in the region remain among the highest in the world and spiked in El Salvador to levels not seen since the country's civil war from 1979 to 1992. The people hardest hit by the drought include most of the region's subsistence farmers, who constitute 25 to 40 percent of the population in Guatemala and Honduras. The prolonged drought will probably affect 3.5 million people in the region in 2016.

Cuba

Cuban leaders will remain focused on preserving political control as they prepare for a probable presidential transition in 2018. Economic reforms to reduce the state role in the economy and promote private economic activity will continue at a slow pace, in part because of probable resistance from senior leaders and government officials concerned that rapid changes might provoke popular unrest. Living standards will remain poor. Along with fears among the Cuban population that the United States will repeal the 1966 Cuban Adjustment Act, the statute allowing Cuban nationals to apply to become lawful permanent US residents, these trends sustain the increasing migration of undocumented Cubans. Migration is particularly acute across the US southwest border where 31,000 Cubans crossed in FY2015, a 76-percent increase over the prior year.

Venezuela

The opposition alliance won a much-coveted majority in the December 2015 national assembly elections, setting the stage for a political showdown in 2016 between the legislative and executive branches. The opposition will seek to implement its policy agenda, which might include pursuing a presidential recall referendum. Economic issues will also figure prominently on the domestic agenda for 2016. Caracas will probably encounter fiscal pressures as it seeks to avoid a default on its sovereign debt in 2016; the economy is suffering from a severe recession that the IMF projects will cause it to contract by at least 8 percent in 2016. Venezuela's government has declined to release complete official figures on macroeconomic indicators, such as inflation and growth.

Brazil

Brazil's investigation into corruption at state-controlled oil company Petrobras will probably continue through 2016. Scores of Petrobras officials, construction firm executives, and politicians have been jailed since the probe was launched in March 2014. Brazil lost its investment-grade rating in December 2015 after the second credit agency in three months downgraded the country's debt to junk status. Further damaging revelations from the probe might prolong political gridlock in Brazil. Meanwhile, preparations are underway in Brazil to address infrastructure, logistics, and security issues involved in hosting the 2016 Summer Olympics in Rio. Organizers are using past Olympics as models, cooperating with foreign governments, and building upon Brazil's experience organizing a large and sustained security posture such as when it hosted the World Cup in 2014.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Ms. Kathleen McGettigan
Acting Director
U.S. Office of Personnel Management
Questions from Representative Stacey E. Plaskett
Committee on Oversight and Government Reform
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. At the hearing, I asked "which or any of the senior White House staffers who have access to [classified] materials are under criminal investigation by the FBI?" In response to that question, you stated, "We will get back to you." As a follow-up to my question, please answer the following:

    a. Are there currently any senior officials working in the Trump Administration who are being afforded access to sensitive or classified information and are under investigation by the FBI? If so, how many individuals, and who are they?

Response: Requests for background investigations for presidential appointees under the purview of the Executive Office of the President (EOP) are generally submitted to the Federal Bureau of Investigation (FBI), which is EOP's cognizant investigative service provider (ISP), not to OPM. Thus, OPM is not aware whether senior officials working in the Administration who have been afforded access to sensitive or classified information are under investigation by the FBI.

    b. Have any former senior officials within the Trump Administration been provided access to sensitive or classified information while under investigation by the FBI? If so, how many individuals, and who are they?

Response: Requests for background investigations for presidential appointees under the purview of the Executive Office of the President (EOP) are generally submitted to the FBI, which is EOP's cognizant investigative service provider (ISP), not to OPM. Thus, OPM is not aware whether former senior officials within the Administration who had been afforded access to sensitive or classified information were under investigation by the FBI.

    c. Do any current White House staff have previous criminal convictions? If so, how many staffers? Please provide the names of the staffers, their titles, and what the previous criminal conviction was for.

Response: Requests for background investigations for White House employees under the purview of the Executive Office of the President (EOP) are generally submitted to the FBI, which is EOP's cognizant investigative service provider (ISP), not to OPM.

d. Are any White House staff under active investigation by the FBI or other law enforcement authorities? If so, how many staffers? Please provide the names of the staffers and their titles.

Response: Requests for background investigations for White House employees under the purview of the Executive Office of the President (EOP) are generally submitted to the FBI, which is EOP's cognizant investigative service provider (ISP), not to OPM.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. David DeVries
Chief Information Officer
U.S. Office of Personnel Management
Questions from Chairman Jason Chaffetz
Committee on Oversight and Government Reform
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. What kind of notifications is the IT security team required to make before deploying security tools onto the network?

    a. If so, what is the purpose of these notifications?

Response: Based on the wording of these questions, as a whole, we are interpreting the phrase "notifications" in this question to mean notifications to employees and employee representatives (unions).

We consider the legal question of whether an agency is required to notify and bargain with union representatives prior to making changes in the area of information security to be unsettled. So far, this has not affected OPM's timely deployment of security tools.

2. Have you seen the deployment of such tools delayed because of the need to notify union representatives?

Response: Not at this point in time.

3. What kind of barriers or challenges have you seen in trying to timely deploy security tools?

Response: As yet, none.

4. Are there any other administrative or regulatory or bureaucratic barriers at OPM that prevent or delay your work the timely deployment of such tools?

Response: A 2014 administrative decision (*U.S. DHS, U.S. ICE*, 67 FLRA 501) of the quasi-judicial, three-member, presidentially appointed and Senate-confirmed Federal Labor Relations Authority may have created potential obstacles to delay timely deployment at agencies. So far, this has not affected OPM's timely deployment of security tools. Additionally, the need for resources may, at times, cause an increase in the time for deployment of security tools, however these have not been significant delays and often the

reallocation and prioritization of resources within the Office of the Chief Information Officer can resolve the issue.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. David DeVries
Chief Information Officer
U.S. Office of Personnel Management
Questions from Chairman Will Hurd
Subcommittee on Information Technology
Committee on Oversight and Government Reform
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

Series I

1. What is OPM's plan to boost capacity in order to decrease the growing backlog of background investigations (and subsequently decrease average investigation time) and how quickly will this plan be implemented?

Response: Capacity to conduct investigations is not restricted by IT. As for the National Background Investigation Bureau's (NBIB) efforts to boost its capacity to decrease the backlog of investigations, it is my understanding that Director Phalen has provided answers in response to Chairman Chaffetz in his Questions for the Record outlining in detail NBIB's efforts to grow their capacity. I defer to Director Phalen to speak for NBIB in this respect.

2. What are the top impediments to achieving this plan and being successful?

Response: I agree with Director Phalen's response to Question 11 from Chairman Will Hurd in the Questions for the Record Director Phalen has submitted in connection with this hearing.

3. What could be done to considerably accelerate the implementation of this plan?

Response: Each aspect noted in Director Phalen's responses is a continuous and ongoing effort for NBIB to meet agencies' needs. NBIB has met with its contractors to receive their plans on increasing their staff to apply to this work and will continue to encourage new capacity growth. Additionally, NBIB has implemented initiatives to reduce the time needed to onboard these vital resources and will continue to look for additional efficiencies.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Series II

1. Who do you report to at the agency?

    a. Who does your performance review?

Response: The OPM Director.

    b. How often do you meet with the head of the agency?

Response: I report directly to the OPM Director (currently Acting Director) with whom I meet individually at least once a week. I also meet with her in a larger forum at least three times per week during meetings with Office of the Director leadership and the direct report Agency leaders.

2. Do you currently have authority in practice to review and manage the IT portfolio for the entire agency? Why/not?

Response: As the co-chair of the Investment Review Board (IRB), which is one of OPM's governance boards, I review and provide recommendations for the approval of IT investments. The IRB was re-constituted in August 2016 and is now actively reviewing IT investments above $250,000. As a voting member of the OPM Capital Investment Committee board, I review and approve acquisition requests in excess of $250,000, and I specifically flag those involving procurements for IT services or capabilities. Since my arrival at OPM in September 2016, my visibility has grown over the OPM IT portfolio. This has been fostered by the implementation of an IT Acquisition Review Checklist. This review encompasses IT spending by the agency in amounts over $250,000. Additionally, the CIO office has initiated IT portfolio reviews of all recorded IT investments, both major and non-major.

    a. What are the challenges?

Response: There are a variety of challenges that may impact my ability to review and manage the OPM IT portfolio. Already, I have incorporated best practices to review the large value procurements – which have added a level of formality and a degree of rigor that is more effective. Currently, OPM Leadership is working through organizational structures, the variety of funding mechanisms, and the nature of procurement reviews to better align contract vehicles and improve agile development and delivery of effective and secure capability.

3. Have you completed an annual IT investment portfolio review?

    a. Could you provide examples of where you identified opportunities to reduce waste and duplication - or create efficiencies as a result of this review?

Response: Since arriving at OPM in September 2016, I have begun to execute IT portfolio reviews. To date, we have executed comprehensive reviews for the NBIB IT Programs, and initial reviews of financial management systems and retirement services systems. The reviews for the NBIB systems resulted in agreed upon priorities and work required for FY 2017, and additional efforts that will be executed by the Department of Defense on the National Background Investigation Services (NBIS) effort in concert with OPM maintaining and operating the legacy capability for the foreseeable future.

OPM will complete a full review of its IT portfolio in 2017, which we anticipate will better position us to identify opportunities to reduce waste/duplication and create efficiencies. I reviewed all major IT investments for FY17 and FY18 and posted these to the IT Dash Board in May 2017 as part of the annual budget submission to OMB.

4. Do you approve the IT budget request of your agency?

    a. How does this review process work?
    b. Describe how the CIO and the CFO manage IT budget coordination.

Response: The Chief Financial Officer (CFO) and I work in close coordination on the initial IT budget requirements planning and IT budget formulation, and we also approve the Agency IT Budget request. The process is as follows: the CFO and I review the IT Portfolio Summary, which includes, what was previously known as the Office of Management and Budget (OMB) Exhibit 53 and the IT Business Cases, before submission to OMB around September of each year. Then, the CFO and I again review the IT budget in conjunction with OMB.

5. Are you certifying that IT investments are delivering functionality on an incremental basis (within six months)? Please provide an example.

Response: I oversee the certification of incremental development through an integrated IT Program Manager and business function team. OPM uses the stage gate review process to evaluate the Major IT Business Cases for compliance with this requirement. As an example, during FY 2016 a major undertaking was the USAJOBS investment and incremental development. This project delivered incremental functionality every two to six months, resulting in a significantly more user-friendly capability and wider customer acceptance. This is a nascent capability and is being applied as contracts are initiated or renewed.

6. Do you review and approve IT contracts on a Department-wide basis?

    a. Have you recently terminated any IT contracts due to cost growth, schedule delays or other factors?

Response: The Office of Procurement Operations (OPO) executes contract pre-award, award, and post award activities; it is the office with procurement authority within OPM. As CIO, I utilize a process to review and approve IT Acquisition Checklist requests for contract actions over $250,000 prior to acquisition, with the goal to increase visibility into IT related contract actions. OPO requires an approved IT Checklist signed by the CIO before it will execute contract activities.

Since arriving at OPM in September 2016, I have not recommended that OPO terminate any IT contracts. I have consolidated duplicative contract requirements.

7. Are you familiar with the term TechStat? Have you conducted any TechStat reviews since you've been at the agency?

Response: I am familiar with the term TechStat; I have conducted several Quarterly Program Reviews (QPRs) on programs at OPM, which are analogous to TechStat reviews.

8. What is your role in the hiring and performance reviews for other agency IT employees?

    a. Do you approve the appointment of other agency IT employees?

Response: I conduct the performance reviews for my direct reports, and I approve the hiring selections of CIO employees.

9. What plan or strategy does your agency have in place to recruit and retain IT talent?

Response: OPM's Office of the Chief Information Officer (OCIO) actively participates in IT forums and speaking engagements across the Federal workspace and participates in various government-wide programs that kicked off in FY 2016 to recruit and retain IT talent. To further our retention efforts, OCIO held cyber workforce orientation training for the program. Additionally, the OCIO provided training opportunities in Agile and Information Technology Infrastructure Library Certifications to attract and retain IT and Cyber professionals. Our goal is to enhance training and certifications for our technical workforce. This includes providing a minimum number of hours of training for each employee each year.

10. Does your agency have a human capital plan for address supporting timely and effective IT acquisition?

Response: OPM prepares an acquisition human capital plan which includes an IT Supplement. This plan is submitted annually to OMB, in accordance with OMB requirements.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
Questions from Chairman Jason Chaffetz
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. As of February 1, 2017, what is NBIB's current backlog of Initial and Periodic Reinvestigation background investigations and adjudications?

Response: As the primary Investigative Service Provider for the government, the National Background Investigations Bureau (NBIB) provides investigations to Federal agencies, which, in turn render adjudicative decisions based upon the investigation, any other pertinent information (such as polygraphs when applicable), and the adjudicative criteria for the particular type of decision rendered (*e.g.*, eligibility for access to classified information, suitability for Federal employment, etc.). Because NBIB does not conduct adjudications, they are not considered to be part of NBIB's processes and/or the current inventory referenced in the chart below.

As of February 1, 2017, there were 554,437 cases in our current inventory. What follows is a breakdown of the case types by category.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Pending Current Inventory*

As of: 2/1/2017

Initial	352,047	Reinvestigation	187,418	Other	14,972
National Security	**244,530**	**National Security**	**173,333**		
SSBI	70,206	SSBI-PR	9,089	ASI	13
Tier5	17,458	Phase PR	36,772	MFI	3
ANACI	402	Tier5R	30,516	NAC	6,685
NACLC	2,005	Tier3R	66,956	RSI	4,497
Tier3	154,459			SAC	3,772
				SACI	2
Suitability/Fitness / Credentialing	**107,517**	**Suitability/Fitness/ Credentialing**	**14,085**		
NACI	1,516	Tier2RS	6,172		
Tier1	35,718	PRI	5,051		
MBI	11,909	Tier4R	2,862		
Tier2S	38,563				
BI	14,959				
Tier4	4,852				

**Note:* *Volumes provided are simply the pending case volume (inventory on-hand). Not all these cases should be considered "backlog" as it is normal to have some cases pending at any given point in time. NBIB's long-term goal is to reduce pending inventory to 160k to 180k cases at any time, a level that can be processed with current workforce capacity.*

2. Regarding the backlog, how are you prioritizing the case types which are addressed first?

Response: As a general rule, NBIB assigns cases based on the oldest case due date, with initial cases being the primary focus.

NBIB works with customer agencies, however, to identify high risk populations, or individuals with special circumstances, which require expedited service. NBIB staff meets with customer agencies routinely to understand their needs and, in some instances, creates special processes to flag cases for prioritization.

NBIB is committed to working with our customers to address their needs and investigations as quickly as possible.

3. How old is the oldest pending case?

Response: There are currently 21 cases that are greater than 1,000 days old, with the oldest being 1,300 days old. Cases falling into this category are generally awaiting a response from a third party record provider, preventing the case from closing. In most of these situations, the third party record provider has a separate pending/ongoing investigation (e.g., potentially criminal) on the subject of the NBIB investigation. In an effort to avoid jeopardizing the ongoing investigation, the third party record provider will not release a final result to NBIB until the investigation is complete. Occasionally, the cases are pending a subject interview which cannot be completed due to the extenuating circumstance of the subject being out of the country for extended periods of time in a location that is not conducive to interview. In cases like these, NBIB makes customer agencies aware of the pending investigative lead and these agencies have the ability to view or request a copy of the partially completed investigation. The customer agency can use the partially completed investigation to inform an adjudicative decision or to discontinue the investigation if it is no longer needed.

4. In January 2017, NBIB increased the interval of security clearance reinvestigations from 5 years to 6 years in an effort to reduce the backlog of pending open cases.

    a. Is this really the right way to reduce the backlog?

Response: NBIB does not have the authority to amend the interval for security clearance reinvestigations and did not take this action. The Director of National Intelligence, in his role as the Security Executive Agent, is responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to the determinations by agencies of eligibility for access to classified information or eligibility to hold a sensitive position. For additional information pertaining to the periodicity of reinvestigations, NBIB defers to the Office of the Director of National Intelligence (ODNI) for current policy and guidance issued to agencies.

    b. Doesn't this potentially create a security vulnerability?

Response: The Director of National Intelligence, in his role as the Security Executive Agent, is responsible for developing uniform and consistent policies and procedures to ensure the effective, efficient, and timely completion of investigations and adjudications relating to the determinations by agencies of eligibility for access to classified information or eligibility to

hold a sensitive position. For additional information pertaining to security vulnerabilities associated with such policy changes, NBIB defers to ODNI.

5. What other alternatives have you considered to reduce the backlog for reinvestigations?

Response: Since 2016, NBIB has been growing capacity in order to apply more resources and productive hours to the workload. The investigative workforce of Federal employees has grown from 1,300 investigators in 2014 to over 1,500 today, with a target level of approximately 2,000 Federal investigators by FY18. Further, NBIB continues to shift resources and apply overtime where applicable to combat growing workload bubbles by locality and identify efficiencies where applicable. For example, since April 2016, 311 Federal investigators have traveled outside their permanent duty stations in support of localized surges.

In addition, we have worked with our vendors to grow new capacity to approximately 4000 contractor field investigative staff to devote to this workload. The contract vendors are also recruiting new staff and have many new investigators in their hiring and training pipeline.

However, the ramp up time for new investigators can be extensive, because these investigators must themselves undergo rigorous vetting and must complete a training program under national investigative training standards, through an accredited training course and on-the-job training.

We have also implemented a number of efforts to thoughtfully reduce the level of effort required to complete investigations and increase our efficiency, ultimately increasing the production from our investigative resources. For example, NBIB has:

- Implemented a new writing style, Focused Report Writing, to reduce the amount of time spent writing reports. The initiative reduces typing time by focusing the writing on adjudicative material and eliminating unnecessary information. It redirects time to active investigation, thereby improving efficiency.
- Revised telephonic interview guidance to allow more flexibility without impacting quality.
- Worked closely with its customer agencies to enable greater scheduling of geographically-centralized interviews to reduce travel time as much as possible, and to expand interviews via video teleconference (VTC) where no known derogatory information exists.

- Implemented all five tiers of the 2012 Federal Investigative Standards, in accordance with the Initial Operating Capability (IOC) jointly issued by the ODNI (as Security Executive Agent) and OPM (as Suitability Executive Agent), and is currently working to convert certain legacy case types in our inventory to the new standards as directed by the Director of National Intelligence to refine the level of effort.

6. What percentage of the 569,000 backlogged cases do you expect to have completed by FY 2018?

Response: As of February 1, 2017, NBIB's current inventory is 554k investigations. After climbing throughout FY 2015-16, this inventory level has remained relatively stable since Q1 FY 2017. From the start of FY 2017 (October 1, 2016) through February 1, 2017, NBIB has closed 808k investigations. This would put NBIB on pace to complete approximately 2.4M investigations by the end of FY 2017.
At the same time, new case requests continue to come in at a steady pace, roughly equal to our completion rate, which will therefore still leave NBIB with a significant inventory as we enter FY 2018. We continue to increase capacity by applying more resources and productive hours to the workload, in an effort to reduce the open inventory to a long-term target level of 160k to 180k cases.

7. Will you have one or two of the vendors starting with the oldest cases and moving forward?

    a. How are you going to spread out the work to ensure the backlog is drawn down efficiently?

Response: The incumbent contractors, CACI and KeyPoint, received their initial case load under the new contracts on February 1, 2017. CSRA received its initial cases on February 16, 2017. Securitas is expected to begin taking cases after completion of the System Security Authorization and Accreditation process, which is anticipated to be completed by May 1, 2017.

As new capacity is added to the program, the workload is analyzed in a manner to determine the most effective and efficient way to utilize the available capacity to complete the cases based on the priorities. Further, in accordance with NBIB's prioritization strategy addressed in an earlier question, the oldest workload is generally being assigned first with a focus on initial cases.

8. How many field investigators over the four vendors, and including NBIB staff investigators, does NBIB have available to address the outstanding number of investigations?

Response: As of March 27, 2017, NBIB has a Federal investigative workforce of 1514 full-time equivalents (FTE). In addition, 118 individuals are in training class or in on-the-job training. NBIB is in the process of hiring additional investigators over the next several months, with a target of 1975 total Federal investigators.

As of March 27, 2017, NBIB's contractor field investigative staff, as reported by the contract vendors, consists of approximately 4058 FTE. The contract vendors are also recruiting new staff and have many new investigators in their hiring and training pipeline.

9. It has been reported that each vendor is guaranteed $1M under the existing contracts. Are there award fees associated with these contracts?

Response: The fieldwork contracts are structured as indefinite delivery indefinite quantity contracts as defined in the Federal Acquisition Regulation. The contracts do not contain an award fee.

10. By the terms of the contracts, how many cases is each vendor expected to complete per month?

Response: The contract is structured to require quality cases to be delivered within specific timeliness standards for each case type. Each company's performance under the contract is based upon how many cases meet those standards and not based upon the number of cases produced. However, the contract sets a maximum ceiling of "units of work" (UOW) that can be ordered monthly from each vendor. Each case type ordered requires a different amount of UOW to complete, so the maximum UOW under the contracts does not specifically correlate to a set number of cases to be completed each month.

11. Has NBIB implemented all of the tiers of the 2012 Federal Investigative Standards when conducting background investigations?

Response: Yes, NBIB has implemented tiered investigations under the implementation plan developed by the Director of National Intelligence as the Security Executive Agent and the Director of OPM as the Suitability Executive Agent for the 2012 Federal Investigative Standards. While all of the tiers have been implemented, the phased implementation plan specifically calls for IOC, to be followed by Full Operating Capability (FOC). The IOC date

for Tiers 1 and 2 was October 1, 2014; for Tier 3, the IOC date was October 1, 2015; and Tiers 4 and 5, the IOC date was October 1, 2016. FOC is scheduled for October 2017.

a. If no, why not?

Response: Not applicable.

12. Has there been an increase or decrease in the number of days to complete an investigation since the implementation of the final tiers of the 2012 Federal Investigative Standards on 1 October 2016?

Response: Although our overall timeline numbers have increased slightly, we do not believe this is a direct result of the new tiered structure. The increase in time is largely affected by older cases being worked out of the inventory and not necessarily a result of a processing time increase related to the tiered structure.

Note - Implementation of the FOC of the Federal Investigative Standards is scheduled for October 2017.

13. Has NBIB implemented a Continuous Evaluation solution for clearance holders under its jurisdiction?

Response: Yes, NBIB is able to offer customer agencies today a continuous evaluation (CE) product that satisfies the guidance issued by the Director of National Intelligence in his role as the Security Executive agent. In this role, the Director of National Intelligence established a phased implementation approach for CE. NBIB will continue to expand coverage to fulfill future requirements and guidance issued by ODNI.

a. If no, why, and when do you expect to implement?

Response: Not applicable.

b. If yes, what databases are being checked in the continuous evaluation, and are the checks automated?

Response: NBIB's CE information collection product is fully automated. The databases to be checked for the initial phase of CE are not identified in the Federal Investigations Notice (FIN) 17-03, and this information has not been made available for public release. NBIB

defers to ODNI for any further response relating to the information regarding database checks.

14. Will the implementation of Continuous Evaluation reduce the volume of Periodic Reinvestigations?

Response: The Director of National Intelligence, in his role as the Security Executive Agent, has not issued a policy allowing agencies to reduce requests for periodic reinvestigations (PR) or to change the frequency of PR based on their implementation of CE. Additionally, current statutes and presidential executive orders treat PRs and CEs as distinct, yet complementary, requirements. *See* 5 U.S.C. 11001(c)(6) (enhanced personnel security programs, including automated record checks of covered persons, are to be "in addition to" the periodic reinvestigations described in the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. 3341); E.O. 12968, as amended, sections 3.4 and 3.5 (separately requiring periodic reinvestigations and continuous evaluations); *see also* E.O. 13467, as amended, section 1.3(q).

15. If Continuous Evaluation is to be an automated process, wouldn't there still be a need for human analysis of the "hit"?

Response: As noted above, NBIB does not render the adjudications that result from investigative inquiries. Thus, although NBIB's CE information collection product is fully automated, agencies receiving the results are still required to adjudicate the information. Information received from record searches will be reviewed by customer agencies to determine if any additional investigative work (e.g., automated record checks or interviews) is warranted prior to the agency adjudicating the investigation. During the adjudication process, human analysis is required to render a determination for continued eligibility for access to classified information or continued eligibility to hold a sensitive position.

a. What will be the required response time for adjudicating a hit?

Response: The adjudication of a hit is the responsibility of the requesting agency. In accordance with E.O. 13467, as amended, ODNI is responsible for issuing guidelines and instructions to Federal agencies for effective, efficient, and timely adjudications.

16. Under Continuous Evaluation, what is the anticipated amount of hits per day or week, and have policies been established to address how to respond?

Response: Since the CE is a recent offering and not all agencies are yet utilizing this capability, it is too early to anticipate the amount of hits. As part of the CE, policies have been established to provide requesting agencies with results of any hits.

17. Have there been any clearance holders identified during Continuous Evaluation that posed physical danger to the workforce?

Response: NBIB's product was recently offered to customer agencies to satisfy ODNI's CE (Phase 1) requirement by September 2017. NBIB has received limited requests as of this time, and, therefore, has not yet identified individuals posing a threat to the workforce. We defer to agencies on the outcome of their adjudications.

a. If yes, please provide a summary of what issue was discovered and the action taken.

Response: Not applicable.

18. Does NBIB have a process or procedure to verify that clearance seekers and holders are in compliance with filing federal income tax returns?

Response: Yes, NBIB does have a procedure in place with the Internal Revenue Service (IRS), which is both labor intensive and manual, that we perform on cases where a tax concern is raised during the course of an investigation. However, a process that would enable the ability to conduct searches on all clearance seekers, as defined by the 2012 Federal Investigative Standards, is not yet in place. The requirement is identified as a deliverable for FOC. NBIB, in coordination with the Performance Accountability Council, the Suitability Executive Agent and the Security Executive Agent, is currently working with the Internal Revenue Service to satisfy this new requirement. In the interim, NBIB will continue to conduct credit record searches in accordance with both legacy and new Federal Investigative Standards, which is an additional way that information about tax compliance can arise.

19. How is security clearance reciprocity accomplished?

Response: The Director of National Intelligence, in his role as the Security Executive Agent, is responsible for the issuance of policies, development of metrics and conduct of oversight regarding reciprocity processes for security clearances. Current polices provide that

background investigations and adjudications for security clearances shall be mutually and reciprocally accepted by all agencies (*see e.g.*, 50 U.S.C. 3341(d), Executive Order 13467, as amended, and the 2012 Federal Investigative Standards), unless otherwise authorized by law. Prior to submitting an investigation to NBIB, agencies are required to validate the need for the investigation, reciprocally accept another agency's investigation, if one exists within scope; and reciprocally accept the security clearance determination, unless there is an exception code associated with the adjudication or the agency is aware of new information that has not yet been adjudicated. NBIB defers to ODNI for additional guidance pertaining to the reciprocity policies for security clearances. In contrast, OPM, as Suitability and Credentialing Executive Agent, prescribes reciprocity policy for suitability and identity credentialing.

20. How long does a reciprocity request take to process for each level of clearance?

Response: The Director of National Intelligence, in his role as the Security Executive Agent, is responsible for the issuance of policies, development of metrics and conduct of oversight regarding reciprocity processes for security clearances. NBIB's customer agencies are responsible for determining whether their applicants may access classified information or hold a sensitive position, based on investigations provided by NBIB. NBIB defers to ODNI for additional information pertaining to reciprocity-related measures and metrics for security clearances.

21. Is there an executive branch time requirement for how long these requests should take?

    a. Is it hours, days, weeks?

Response: NBIB defers to ODNI for additional information pertaining to reciprocity policies for security clearances.

22. The ODNI published a document entitled, "Strategy and Schedule for Security Clearance Reciprocity" in April 2014. Among other actions, a reciprocity policy was supposed to be issued in FY 2015. Did this occur?

Response: NBIB defers to ODNI for additional information regarding this policy.

    a. What guidance does NBIB utilize in order to comply with reciprocity requirements?

Response: NBIB utilizes policies and guidance issued by ODNI. Prior to submitting a request for an investigation to NBIB, agencies are required to check all three clearance repositories to determine if an investigation already exists. If there is an existing in-scope investigation and adjudication on file, agencies are required to reciprocally accept the determination, allowing it is not flagged with an exception code. If NBIB learns there is an existing investigation or adjudication on file and eligible for reciprocity, NBIB will bring this to the customer agency's attention so that the customer agency can comply with ODNI's current reciprocity policies and guidelines.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
Questions from Ranking Member Elijah E. Cummings
Committee on Oversight and Government Reform
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. What types of security risks are posed when classified information or government business is conducted over an unsecured electronic network or device?

Response: The use of unsecured communication systems to transmit classified information would present a risk of adversary collection or unauthorized disclosure of classified information, and is prohibited by Executive Order 13526: Classified National Security Information.

2. If the National Background Investigations Bureau (NBIB) discovered that an individual with a security clearance was using an unsecured electronic network or device, what would it do?

Response: If it were determined during the course of the investigation that an individual with a security clearance or an individual for whom a sponsoring agency is considering for the new security clearance used an unsecured electronic network or device to transmit classified or sensitive information, either intentionally or unintentionally, the investigator would gather information to identify the extent of possible unauthorized disclosure, circumstances involved, individuals involved, and other information needed. This information would be provided to the customer agency as part of the completed investigation to inform the agency's determination whether or not the individual should obtain or retain a security clearance. In the event the individual is currently engaging in such behaviors, or if NBIB discovered past events that raised serious concerns, NBIB would immediately notify the sponsoring agency so that necessary actions could be taken, which could include removing the individual from access pending completion of the investigation.

3. Please provide copies of any policies or regulations related to the use of unsecured networks or devices to transmit classified information or conduct general government business.

Response: OPM is aware of regulations at 32 C.F.R. Part 2001 – Classified National Security Information – that address transmission of classified documents, and to which OPM

adheres. OPM also adheres to Executive Order 13526: *Classified National Security Information*, prohibiting the transmission of classified information on systems that are not designated national security systems or approved to process and store information at the appropriate level of classification.

For the systems conducting unclassified general government business, OPM follows the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and Technology (NIST) standards and guidelines for protection of information and information systems.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
Questions from Chairman Will Hurd
Subcommittee on Information Technology
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

Issue: Contractor Capacity
At the end of fiscal year 2016, there were 569,000 cases backlogged at OPM. In September 2016, OPM awarded contracts to four contractors to conduct background investigations. OPM awarded background investigation contracts to four contractors (two incumbents and two new contractors)- reportedly in an effort to increase capacity and address the backlog. OPM said in the September 2016 contract announcement that the new contractors were expected to be operational by December 1, 2016.

1. What is the base period and what are the option periods for this contract?

Response: The contracts are structured with a base and three option periods, which represent ordering periods in which NBIB can issue task orders. NBIB assigns cases under the terms of those task orders. The following are the base and optional ordering periods:

Base Period: December 1, 2016 through September 30, 2018

Option 1: October 1, 2018 through September 30, 2019.
Option 2: October 1, 2019 through September 30, 2020
Option 3: October 1, 2020 through September 30, 2021

2. When did the contract period begin?

Response: The contract period began December 1, 2016. NBIB issued the first task orders to CACI, KeyPoint, and CSRA on January 30, 2017, and assigned the initial case load to CACI and KeyPoint on February 1, 2017. NBIB assigned the initial case load to CSRA on February 16, 2017. NBIB extended the first task orders with CACI, KeyPoint, and CSRA, and issued the first task order to Securitas, on March 30, 2017. NBIB assigned the initial case load to Securitas on April 21, 2017, after Securitas secured an authorization to operate on April 18, 2017.

3. Were the new contractors operational and working cases on December 1st?

Response: No.

a. If not, why not?

Response: In an effort to enhance the protection of the government investigative data, the OPM Chief Information Officer directed contract IT security requirements which were fully vetted and finalized by December 22, 2016. This resulted in the contractors delaying the purchasing of their laptops and finalizing the security protocols for their contractor systems. Once the revised process and requirements were finalized, the contractors quickly moved to purchase hardware and proceed forward with their contractor systems.

b. Who has the final authority to authorize these contractors to begin operations?

Response: The Contracting Officer, based, in part, on the input from the OPM Office of the Chief Information Officer and the NBIB program office, has the authority to permit the contractors to begin operations.

c. When will these two new contractors to be operational?

Response: CSRA is operational and began taking case assignments on February 16, 2017. Securitas received their System Security Authorization and Accreditation on April 18, 2017, and received their first case assignments on April 21, 2017.

4. How many cases have the incumbent contractors received and processed each month since the beginning of this new contract?

Response: From February 1, 2017 to April 30, 2017, the incumbent contractors have received the following number of cases:

KeyPoint - 25,141 (6,303 in February; 7,840 in March; 10,998 in April) cases

CACI - 17,352 (5,255 in February; 5,543 in March; 6,554 in April) cases

During that same period, the incumbent contracts submitted the following cases:

KeyPoint - 36,187 (10,543 in February; 12,492 in March; 13,152 in April)

CACI - 27,124 (8,092 in February; 9,811 in March; 9,221 in April)

5. How many cases have the new contractors received and processed each month since becoming operational?

Response: CSRA is still in the midst of on-boarding into the program but has received 2,286 cases and completed 1,461 as of April 27, 2017. Securitas received their first load of 235 cases on April 21, 2017, after achieving ATO on April 18, 2017.

6. Under the terms of the contract how many cases are contractors expected to receive and process each month?

Response: The contract is structured to require quality cases to be delivered within specific timeliness standards for each case type. Each company's performance under the contract is based upon how many cases meet those standards and not based upon the number of cases produced. However, the contract sets a maximum ceiling of "units of work" (UOW) that can be ordered monthly from each vendor. Each case type ordered requires a different amount of UOW to complete, so the maximum UOW under the contracts does not specifically correlate to a set number of cases to be completed each month.

7. How many field investigators does OPM have available to address the outstanding number of investigations? Please provide the number of field investigators by contractor and Federal employees.

Response: As of March 27, 2017, NBIB has a federal investigative workforce of 1514 full-time equivalents (FTE). In addition, 118 individuals are in training class or on-the-job training. NBIB is in the process of hiring additional investigators over the next several months, with a target of 1975 total federal investigators.

As of March 27, 2017, NBIB's contractor field investigative staff, as reported by the contract vendors, consists of approximately 4058 FTE. The contract vendors are also recruiting new staff and have many new investigators in their hiring and training pipeline.

8. Given the currently available contract and federal resources, by when do you expect to have made progress in addressing the current backlog?

Response: As of February 1, 2017, NBIB's current inventory is 554k investigations. After climbing throughout FY 2015-16, this inventory level has remained relatively stable since Q1 FY 2017. From the start of FY 2017 (October 1, 2016) through February 1, 2017, NBIB has

closed 808k investigations. This would put NBIB on pace to complete approximately 2.4M investigations by the end of FY 2017. Given this statistic, there is a high likelihood that all backlogged cases from the beginning of FY 2017 will be completed by FY 2018.

At the same time, new case requests continue to come in at a steady pace, roughly equal to our completion rate, which will therefore still leave NBIB with a significant inventory. We continue to increase capacity by applying more resources and productive hours to the workload, in an effort to reduce the open inventory to a long-term target level of 160k to 180k cases.

9. What is OPM's plan for prioritizing the processing the backlog of cases?

Response: As a general rule, NBIB assigns cases based on the oldest case due date, with initial cases being the primary focus.

NBIB works with customer agencies, however, to identify high risk populations, or individuals with special circumstances that require expedited service. NBIB staff meets with customer agencies routinely to understand their needs and in some instances, creates processes to flag cases for prioritization.

NBIB is committed to working with our customers to address their needs and investigations as quickly as possible.

10. How long will each aspect of the plan take to be implemented?

Response: Each aspect noted above is a continuous and ongoing effort for NBIB to meet our customers' needs. We have met with our contractors to receive their plans on increasing their staff to apply to this work and will continue to encourage new capacity growth. Additionally, we have implemented initiatives to reduce the time needed to onboard these vital resources and will continue to look for additional efficiencies. Every aspect noted above has already been implemented and work is being performed to expand each one of those efforts to gain the most benefit across the entire program.

11. What are the top potential impediments to the successful implementation of the backlog reduction plan?

Response: The largest challenge to NBIB in implementing a succesful backlog reduction plan is increasing the field investigative capacity. As noted in previous responses, we have hired approximately 500 federal investigators over the last 18 months and will continue to

hire throughout FY 2017. In addition, we are working with our contract vendors to increase their fieldwork capacity. While not an impediment, a key factor to NBIB's success in reducing the backlog will be the development of a more efficient techinical capability to support the background investigation lifecycle. Pursuant to Executive Order 13467, as amended, we are working with Department of Defense (DoD) to build the National Background Investigations Services (NBIS), a whole government approach and capability to managing the background investigation lifecycle.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
Questions from Representative Stacey E. Plaskett
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. At the hearing, you testified that "the chief of the security office for the White House is the determiner for an individual and the senior White House level having a security clearance." When I asked who is responsible for selecting the White House's chief security officer, as well as the identity of the chief security officer and whether that position is a political appointment, you replied, "I actually don't know right now. I can find that answer." Please answer the following questions:

    a. What is the name of the White House security chief tasked with approving security clearances for White House officials?
    b. Please explain the process for hiring and approving the White House security chief.
    c. Please explain whether the White House security chief is an independent position, career civil service appointment, or a political appointment.
    d. When did the current White House security chief assume the position?

Response: The Executive Office of the President (EOP) is responsible for processing national security clearances for White House personnel. Accordingly, EOP is best suited to answer these questions, and NBIB defers to EOP for further response.

2. At the hearing, you were asked about reports that President Trump met with foreign officials in the presence of family members that did not have security clearances. You testified: "The President has the ability to grant a clearance or grant access to classified information to anyone who they please." Please answer the following questions:

    a. What security risks are presented by having individuals without the appropriate security clearances present for classified meetings or briefings?

Response: The President of the United States manages the system of classifying information by executive order (EO 13526). EO 13526 generally describes the potential damage to the national security associated with an unauthorized disclosure of classified national security

information at three specified levels (Confidential, Secret, and Top Secret). OPM would defer to the Office of the Director of National Intelligence for questions about the adjudicative requirements for eligibility for access to classified information, and to the Justice Department for questions about the legal consequences of unauthorized disclosures of classified information.

b. If an applicant for a security clearance disclosed during a background check that he or she had previously shared information with family members who did not have similar clearances, please explain the steps the NBIB would take with regard to that security clearance applicant.

Response: Following such a disclosure, the investigator would work to identify the extent of the possible unauthorized disclosure, circumstances involved, individuals involved, and other information needed to support the final adjudication. Results of the investigations would be provided to the agency requesting the investigation in connection with the subject's eligibility for access to classified information.

c. How many people working in the White House had their background investigations conducted by the National Background Investigations Bureau (NBIB)?

Response: Background investigations for White House employees under the purview of the EOP are generally submitted to the Federal Bureau of Investigation (FBI), which is EOP's cognizant investigative service provider (ISP), not to OPM.

d. As part of the background check process, does the NBIB check whether an applicant for a security clearance has been charged or convicted of any criminal laws?

Response: Yes, part of the background investigation process includes conducting FBI and Local Law Enforcement Agency checks. The scope of these checks will depend on the level of investigation.

e. Is the NBIB aware of any individuals working in the Trump Administration who were found to have had a prior criminal history and were nevertheless still approved for a background check or a security clearance? If so, please provide the number of individuals, the names of those individuals with their titles, and the name of each individual responsible for approving the background check or security clearance.

Response: Background investigations for White House employees under the purview of the EOP are generally submitted to the Federal Bureau of Investigation (FBI), which is EOP's cognizant investigative service provider (ISP), not to OPM.

f. In instances in which the NBIB learns that a White House staff applicant has been convicted of a criminal violation, what does it do with that information?

Response: As noted above, background investigations for White House employees under the purview of the EOP are generally submitted to the FBI which is EOP's cognizant ISP, not to OPM. NBIB background investigations are conducted in accordance with established investigative policies. Issues are investigated to obtain information such as recency of the event, surrounding circumstances, rehabilitation efforts, and other background information needed to support the final adjudication. Information is documented in the report of investigation and submitted to the adjudicative entity.

g. Who is that information reported to within the Trump Administration?

Response: NBIB is not the ISP for White House employees. This question is better addressed to the FBI.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Questions for Mr. Cord Chase
Chief Information Security Officer
U.S. Office of Personnel Management
Questions from Chairman Jason Chaffetz
Committee on Oversight and Government Reform
February 2, 2017, Hearing: "Improving Security and Efficiency at OPM and the National Background Investigations Bureau"

1. What kind of notifications is the IT security team required to make before deploying security tools onto the network?

   a. If so, what is the purpose of these notifications?

Response: Based on the wording of these questions, as a whole, we are interpreting the phrase "notifications" in this question to mean notifications to employees and employee representatives (unions).

We consider the legal question of whether an agency is required to notify and bargain with union representatives prior to making changes in the area of information security to be unsettled. So far, this has not affected OPM's timely deployment of security tools.

2. Have you seen the deployment of such tools delayed because of the need to notify union representatives?

Response: Not at this point in time.

3. What kind of barriers or challenges have you seen in trying to timely deploy security tools?

Response: As yet, none.

4. Are there any other administrative or regulatory or bureaucratic barriers at OPM that prevent or delay your work the timely deployment of such tools?

Response: A 2014 administrative decision (*U.S. DHS, U.S. ICE*, 67 FLRA 501) of the quasi-judicial, three-member, presidentially appointed and Senate-confirmed Federal Labor Relations Authority may have created potential obstacles to delay timely deployment at agencies. So far, this has not affected OPM's timely deployment of security tools. Additionally, the need for resources may, at times, cause an increase in the time for deployment of security tools, however these have not been significant delays and

often the reallocation and prioritization of resources within the Office of the Chief Information Officer can resolve the issue.