AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

SECURITY CLEARANCE INVESTIGATION CHALLENGES AND REFORMS

HEARING

BEFORE THE

SUBCOMMITTEE ON
GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

OCTOBER 11, 2017

Serial No. 115–41

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

27–761 PDF WASHINGTON : 2018

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

Trey Gowdy, South Carolina, *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
Greg Gianforte, Montana

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
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Jimmy Gomez, California

SHERIA CLARKE, *Staff Director*
ROBERT BORDEN, *Deputy Staff Director*
WILLIAM MCKENNA *General Counsel*
JACK THORLIN, *Deputy Subcommittee Staff Director*
KILEY BIDELMAN, *Clerk*
DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

Mark Meadows, North Carolina, *Chairman*

Jody B. Hice, Georgia, *Vice Chair*
Jim Jordan, Ohio
Mark Sanford, South Carolina
Thomas Massie, Kentucky
Ron DeSantis, Florida
Dennis A. Ross, Florida
Rod Blum, Iowa

Gerald E. Connolly, Virginia, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey

CONTENTS

SECURITY CLEARANCE INVESTIGATION CHALLENGES AND REFORMS

Wednesday, October 11, 2017

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

The subcommittee met, pursuant to call, at 2:01 p.m., in Room 2154, Rayburn House Office Building, Hon. Mark Meadows [chairman of the subcommittee] presiding.

Present: Representatives Meadows, Hice, Jordan, DeSantis, Blum, Maloney, and Norton.

Also Present: Representative Krishnamoorthi.

Mr. HICE. [presiding.] Subcommittee on Government Operations will come to order. Without objection, the chair is authorized to declare a recess at any time.

Today's hearing will cover a topic of great importance. How to ensure security clearance investigations are effective and efficient. We're discussing this now because of the record 700,000 investigation backlog of background investigations throughout the Federal Government.

For would-be Federal or contractor employees awaiting their first clearance, the backlog means they have to wait months before they can start working.

The problem calls for thoughtful analysis and meaningful reform, not knee-jerk reactions and superficial solutions.

Unfortunately, we appear to be on the verge of knee-jerk reaction. Transferring responsibility for the vast majority of clearance investigations, back to the DOD away from the National Background Investigations Bureau.

I say "back to," because in a similar record backlog situation in 2004, DOD gave up the investigation responsibility. Back then, DOD thought it needed to focus on its function of defending the country, so it tasked the Office of Personnel Management with the labor-intensive investigations function.

Today, only a year after the creation of the NBIB, the Senate NDAA contains a provision that would transfer the investigation function back to the DOD.

Though DOD has put out a plan for how it would take over investigations, it has yet to issue much in the way of an argument as to why it should do so. There are much clearer reasons for why it should not.

Standing up a DOD investigation capacity while NBIB is still operating would obviously be duplicative to agencies literally doing

the same thing. NBIB has only recently managed to hire enough contractor investigations to match what the Federal Government could muster in 2014 before a scandal involving one contractor forced OPM to terminate 60 percent of the contractor workforce.

A major shift of resources to DOD would halt the growth and the contractor workforce that is digging the government out of the backlog hole. There is every reason to believe, therefore, that a transfer would worsen the backlog and deprive our Armed Forces of the people they need to function.

At the same time, NBIB is spearheading new reforms in technology and administration to make the process more efficient. The ongoing reform effort could be slowed or abandoned altogether, as DOD spends its institutional energy simply recreating what already exists at NBIB.

The contractor community shares these concerns. The people whose money depends most on a functioning investigation system are telling us not to transfer investigations back to DOD.

I hope today's hearing will help Congress make an informed decision on whether to go ahead with the transfer to DOD through the NDAA process.

I would like to thank our witnesses for being here today and I look forward to hearing from your testimony.

I now would like to recognize the ranking member, Ms. Norton, for her opening statements.

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

Thank you for holding this hearing to examine both the current backlog in the Federal security clearance investigations, and potential reforms to the background investigation process.

Last month, the National Background and Investigations Bureau reported a backlog of approximately 700,000 security applications. This backlog and the lengthy wait time for security clearances is unacceptable.

It is critical that the NBIB address this problem and important for Congress to provide and resolve the necessary resources and support to do so.

Since it first began operating in October 1, 2016, the NBIB has been tasked with the challenge of not only improving the Federal Government's process for conducting background checks, but also bringing down the growing security clearance backlog.

Since its creation, the NBIB has made several enhancements to the security clearance investigation process. For example, it developed a continuous evaluation program for monitoring an employees's or contractor's eligibility to maintain access to classified information. And earlier this year, the NBIB created a new law enforcement unit to improve the government's ability to gain access to criminal history records of State and local enforcement agencies.

This is an important change that could eliminate a critical gap in how background checks were previously conducted. The gap has enabled an unknown number of people to gain security clearances they probably should not have received. The importance of gaining access to criminal history records became all too clear on September 6, 2013 when Aaron Alexis, a Federal contractor, with a se-

cret level clearance entered the Washington Navy Yard, killed 12 people and injured four others.

During the investigation into that incident, we learned that the background investigation of Mr. Alexis failed to identify his history of gun violence.

Local police records of his 2004 firearms arrest had never been provided to Federal investigators. Improving the level of communication between local law enforcement agencies and Federal background investigators can prevent future tragedies like the one at the Navy Yard here in the District of Columbia.

While the NBIB has made some gains in improving the background investigation process, it has struggled to reduce the heavy backlog of security clearance applications.

The current backlog is largely due to termination of the contract that U.S. Investigation Services had with the Office of Personnel Management to conduct background checks. USIS had previously performed the bulk of background investigations for OPM, but was caught defrauding the government on a massive scale, allegedly dumping 665,000 background check cases, indicating to OPM that the background checks had been complete when the proper reviews had not taken place.

OPM had no choice but to terminate the contract with that company. At the time of USIS's termination, it held 60 percent of the Federal Government investigative capacity for background checks. OPM remains unable to fully replace the significant amount of capacity that was lost with USIS's termination, and we need to know why.

Various proposals have been put forward to address the backlog. The most notable of these is the Department of Defense plan that would strip the NBIB of its background investigations for DOD personnel.

Most recently, the Senate has included language in its draft of the National Defense Authorization Act for fiscal year 2018 that would adopt DOD's plan. The DOD plan raises serious concerns. Namely, it could potentially increase, rather than decrease, the existing backlog for security clearances.

According to the DOD plan, it would take the Department at least 3 years to even assume responsibility from the NBIB for background checks of its personnel. During that 3-year transition period, the NBIB would be expected to use its limited resources to help the DOD build the capacity required to perform its own background checks, which may result in additional backlogs at the BIB. The BIB has examined DOD's proposal and found it has potential to, and I quote, "exacerbate the current investigative backlog," end quote.

OPM has also examined DOD's plan and reached the same conclusion. Outside of the Federal Government, policy organizations ranging from the Information Technology Industry Council to the Professional Services Council, have reported that DOD's plan would, and I quote, "cause further delays."

Transferring a significant portion of the NBIB's responsibilities to the DOD also risks returning to a process that was previously found to be inefficient.

Prior to 2005, DOD was responsible for conducting background investigations of its own personnel. During that time, the government accountability office issued a series of reports that raised concerns over the quality and the timeliness of those investigations.

The most significant of those reports was released in 1999 in which the GO found that, and I quote, "DOD personnel security investigations are incomplete and not conducted in a timely manner," end quote.

DOD's failure to adequately handle its own security clearance investigations was a primary reason that responsibility was transferred to OPM in 2005.

Congress needs to seriously examine the best means to reduce the current backlog, but we must do so in a way that balances the need to expedite the process without sacrificing the quality of those investigations.

The Navy Yard shooting, and high profile National Security leaks, such as the one carried by the contractor, Edward Snowden, highlight the need for ensuring that background checks are conducted in a thorough and efficient manner.

I want to thank the witnesses for testifying today. We look forward to hearing from each of you on ways we can strengthen the Federal Government's capabilities when it comes to security clearance investigations.

And I thank you again, Mr. Chairman.

Mr. HICE. Thank you. At this time, I'm pleased to introduce our witnesses.

First, we have Charles Phalen, Jr., the Director of the National Background Investigations Bureau at the Office of Personnel Management.

Next to him is Garry Reid, Director of Defense Intelligence in the Office of Under Secretary of Defense for Intelligence at the Department of Defense.

Next is William Evanina, is that correct?Mr. Evanina is the Director of the National Counterintelligence and Security Center at the Office of the Director of National Intelligence.

And then finally, Mr. Trey Hodgkins, III, Senior Vice President For the Public Sector At the Information Technology Alliance.

I want to thank each of you for being here today. And welcome you all pursuant to the committee rules. All witnesses will be sworn in before they testify. So at this time, if you would please rise and raise your right hand.

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

Mr. HICE. The record will reflect that all witnesses answered in the affirmative, and we appreciate it.

In order to allow time for discussion, please, I would ask that you limit your testimony to 5 minutes, knowing that your entire written statement will be made part of the record.

As a reminder, the clock there in front of you shows your remaining time. When the light turns yellow, you have 30 seconds remaining, and then when it turns red, your time is up. So please, wrap it up as rapidly, as quickly as you can at that point.

And, please, also remember to press the button for your speaker. And I'd ask that you'd put the microphone up there closely right in front of you so we can hear.

So at this time, Mr. Phalen, I'm honored to recognize you for 5 minutes. And thank you for being here.

WITNESS STATEMENTS

STATEMENT OF CHARLES PHALEN

Mr. PHALEN. Thank you, Mr. Chairman, ranking member and members of the subcommittee. I'm Charles Phalen, Jr., and I'm the Director of the National Background Investigation Bureau of the Office of Personnel Management, and I do appreciate the opportunity to appear before you today.

Over the past year, since we stood up on October 1st, NBIB has established a strong focus on National Security, customer service, and continuous process and improvement to meet the critical government-wide need for a trusted workforce.

NBIB conducts 95% of the investigations across the Federal Government, even those few agencies that have delegated or statutory authority to conduct their own investigations, such as some agencies in the intelligence community, rely on NBIB services in some capacity.

Our organizational structure is aimed at leveraging automation to the greatest extent possible, transforming business processes and enhancing customer engagement and transparency. And I strongly believe that these efforts are paving the way for improvements in the efficiency, cost effectiveness and the quality of the investigations in the Federal Government.

I would like to address NBIB's existing investigative backlog, which has been the subject of much attention. The current inventory stabilized this summer and has reduced modestly over the last 10 weeks.

Our current inventory is approximately 704,000 investigative products, including simple record checks, suitability and credentialing investigations, along with the more labor-intensive national security investigations and reinvestigations.

The total number of investigative products is greater than the number of individuals that are waiting for their first security clearance to begin working on behalf of the government.

A significant percentage of individuals waiting for their initial national security investigations are working under interim clearances pending completion of the full investigation and ultimate adjudication.

NBIB has worked to increase capacity and realize efficiencies in as many ways as possible.

Stabilization and modest increases have been attained because we have invested in the necessary infrastructure. This infrastructure has been built through contractor and Federal workforce capacities.

In 2016, NBIB hired 400 new Federal investigators, and awarded a new field work contract doubling our field work contract companies from 2 to 4.

In 2017, we initiated hiring another 200 Federal investigators, issued work under those new contracts, and we are working closely with the vendors to quickly increase the capacity of our contract investigators. We had a goal in 2017, and we missed it by about 6 percent, but we are at, or near the level of contract investigations and Federal investigators that we had in 2014. We have recovered to that level.

As of today, that's a little over 6,900 full-time equivalent investigators working on our behalf. We are targeted to grow that number.

NBIB also believes its capacity can be increased to the smarter use of our workforce's time. The less time each investigator needs to spend on each case, the more time the investigator has for the next case in his or her own queue. This has led us to streamlining processes, reallocating resources and amending our internal policies for greater efficiencies and effectiveness while maintaining quality and reciprocity for all of the government.

Use of investigator time can also be the strengthened through effective use of technology and other available tools. Our efforts have targeted surgical approaches, such as successfully expediting 14,000 cases in accordance with agencies' prioritize list, and done that in an average time of 95 days.

NBIB has actively enhanced customer service and accountability in a number of ways, including realigning price adjustments earlier this fiscal year to better align with agencies' budget cycles.

NBIB is focused on policy and process changes to add efficiency, reduce the level of effort and maintain the investigative quality. And to support this effort, we work closely with the Department of Defense and other customer agencies. We're working to address current challenges and introduce mitigation activities to best serve the interest of all government agencies and departments.

We will, with the support of its interagency partners, make, and will continue to make, improvements on the background process. We have strengthened our partnership with DOD while building the National Background Investigation Services, NBIS, which will serve as NBIB's IT system for the whole of government, to perform background investigations across the spectrum.

As NBIS comes online, we will be able to phase out our legacy systems in favor of NBIS. It is imperative that this mission evolve by leveraging cutting-edge technologies and applying innovative solutions to obtain rich and valid information in support of clearance determinations. It is equally important that the process, improvements, and methodologies have made it across the entire enterprise in a standardized fashion so the quality of investigative products facilitate the reciprocity of clearances across the Federal Government.

As we work to reduce the inventory, we will continue to explore new and innovative ways to meet our customers' needs and leverage their expertise, and remain transparent and accountable to our stakeholders and to Congress.

We recognize that solutions reduce the inventory, and to maintain the strength of the background investigation program, include people, resources and technology.

And thank you again for the opportunity to speak with you here today. I look forward to answering any questions you have.

[Prepared statement of Mr. Phalen follows:]

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

STATEMENT OF

CHARLES S. PHALEN, JR.

DIRECTOR

NATIONAL BACKGROUND INVESTIGATIONS BUREAU

U.S. OFFICE OF PERSONNEL MANAGEMENT

before the

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES

--

October 11, 2017

Chairman Meadows, Ranking Member Connolly, and Members of the Subcommittee, my name is Charles S. Phalen, Jr., and I am the Director of the National Background Investigations Bureau (NBIB) at the Office of Personnel Management (OPM). I appreciate the opportunity to appear before you today.

NBIB was established on October 1, 2016, and is the primary provider of background investigations for the Federal government. Over the past year, NBIB has established a strong focus on national security, customer service, and continuous process improvement to meet the critical Government-wide need for a trusted workforce. In my 36 years working in the Federal security space at the Central Intelligence Agency, the Federal Bureau of Investigation, the National Reconnaissance Office, and industry, I have seen this business through several lenses. I took the position as Director of the NBIB because I believe in its mission and want to make a lasting impact to the personnel vetting processes securing our Nation's most sensitive information, people, and assets.

NBIB conducts 95 percent of investigations across the Federal government. Even those few agencies that have the delegated or statutory authority to conduct their own investigations, such as agencies in the Intelligence Community, rely on NBIB's services in some capacity (e.g.,

Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
--
October 11, 2017

NBIB's electronic questionnaire, national agency record checks, central clearance repository, etc.). Its new organizational structure is aimed at leveraging automation to the greatest extent possible, transforming business processes, and enhancing customer engagement and transparency. I strongly believe these efforts are paving the way for improvement in the efficiency, cost effectiveness, and quality of the investigations across the Federal government.

I would like to address NBIB's existing investigative "backlog," which has been the subject of media attention. The current inventory has begun to stabilize and has even reduced modestly over the last seven weeks. As of September 27, 2017, NBIB's inventory is approximately 707,000 investigative products, including simple record checks, suitability and credentialing investigations, and more labor-intensive national security investigations. The total number of investigative products is greater than the number of individuals that are waiting for their first security clearance to begin working for or on behalf of the Government. Of the total outstanding investigative products, approximately 134,000 are either simple record checks that move in and out of the inventory daily or investigations that support credentialing and suitability determinations. Additionally, approximately 330,000 of NBIB's national security determinations or clearances inventory are for initial investigations and 210,000 are for periodic reinvestigations. A significant percentage of the individuals waiting for their initial national security investigation are working under an interim clearance pending the completion of a full investigation and adjudication.

Looking forward, it is our continued NBIB priority to address the investigative inventory while maintaining a commitment to quality and returning back to the level of performance realized from 2009 through 2014. NBIB is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DoD), and other customers, to focus our efforts in primary areas.

As OPM testified before you earlier this year, in late 2014, OPM's capacity for contract investigation services was drastically reduced by the loss of OPM's largest field contractor, resulting in a loss of productivity, which led to the growth of the pending investigative inventory. This inventory was exacerbated by three unrelated events: 1) the cybersecurity incidents at OPM that were announced in 2015, which necessitated some immediate steps to respond to the incidents and enhance security, e.g., temporarily suspending electronic processing; 2) a higher than expected volume of fieldwork-intensive investigations in Fiscal Year 2016; and 3) concurrent implementation of the 2012 Federal Investigative Standards which required new investigation types and different coverage requirements.

Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
--
October 11, 2017

Understanding the impact these incidents had, in the last year since formation, NBIB has worked to increase capacity and realize efficiencies in as many areas as possible. This stabilization and these modest decreases have been attained because NBIB has invested in the necessary infrastructure. This infrastructure has been built through contractor and Federal workforce capacities. In 2016, NBIB hired 400 new Federal investigators and awarded a new investigative fieldwork contract, doubling the fieldwork contractors from two companies to four. In 2017, NBIB initiated the hiring of another 200 additional Federal investigators, issued work under the new contracts in February, and is working closely with vendors to quickly increase the capacity of contract investigators. As of today, there are over 6,900 full-time equivalent investigators working on behalf of NBIB, a number we are targeting to grow. For context, the Federal and contractor workforce capacity increased by 25 percent to address the current investigative inventory. This allowed NBIB to increase average monthly production by 6 percent in FY2017 for the T3 (secret) and T5 (top secret) population; and 15 percent higher in the last quarter of FY2017 compared to the FY2016 monthly average. As investigators complete training and reach maximum productivity, NBIB's monthly production rate is projected to continue to increase into FY2018.

NBIB also believes that capacity can be increased through smarter use of our workforce's time. The less time each investigator needs to spend on each case, the more time the investigator has for the next case in his or her queue. This has led us to streamline processes, reallocate resources, and amend internal policies for greater efficiencies and effectiveness while maintaining quality and reciprocity for all of Government. This has allowed NBIB to reform traditionally manually-intensive practices and reduce the number of hours each investigator needs to spend on each case. Use of investigator time can also be strengthened through effective use of technology and other available tools. NBIB has improved fieldwork logistics by centralizing and prioritizing cases; increasing efficiencies of Enhanced Subject Interviews (ESIs) and reporting; leveraging video teleconferencing (VTC) for Subjects in remote locations; and using telephonic interviews more liberally when applicable to quickly conduct investigative leads on clean non-issue cases. NBIB has also digitized and automated data, records and information by proactively reaching out to record providers to negotiate direct connections, access to terminals, and revised interagency agreements to more quickly facilitate downstream actions, such as case closings and adjudications.

Our efforts have included targeted, surgical approaches such as successfully expediting 14,000 cases in accordance to agency prioritized lists with an average timeliness of 95 days. NBIB has also made more targeted use of flags to trigger expanded investigations, resulting in the cancellation of unnecessary enhanced subject and converted top secret legacy cases to the new

Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
--
October 11, 2017

Tier 5 investigations for Federal workforce. NBIB has actively enhanced customer service and accountability in a number of ways, including realigning price adjustments earlier in the fiscal year to better align to agencies' budget cycles; serving as a key player on the Background Investigation Rate Council; and establishing a Customer Service Advisory Board to advise me and the agency leadership team.

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 DoD and other customer agencies, conducted a detailed business process reengineering effort and worked in collaboration with ODNI, in its role as the office supporting the Security Executive Agent, to identify appropriate policy and process changes to help address the inventory. NBIB is also working with DoD to build a more secure and more flexible automated case management system that will allow NBIB to implement more efficient and effective case processes. NBIB has helped to establish a new organizational structure with strong interagency representation through full-time employees recruited to OPM from stakeholder agencies as well as through a newly established joint duty program. This organizational structure addresses current challenges and introduces mitigation activities to best serve the interests of all Government agencies and departments, as well as Government-wide reform efforts. The structure will help facilitate NBIB's strategy for reform, which focuses on innovation, risk management, and customer and stakeholder engagement in transformation activities.

NBIB, with support from its interagency partners, has made and will continue to make improvements to the background investigation process. As part of the Performance Accountability Council, NBIB is working together with our interagency partners to develop, implement, and continuously re-evaluate and revise outcome-based metrics that measure the effectiveness of the vetting processes (e.g., security, investigative and adjudicative quality, cost, timeliness, reciprocity, customer service, and other performance characteristics). These efforts include: 1) launching programs to continuously evaluate personnel with security clearances to determine whether these individuals continue to meet the requirements for eligibility; 2) enhancing information sharing among State, local, and Federal Law Enforcement entities when conducting background investigations; and 3) assessing the quality of background investigations using a standard set of rules and an automated tool. Additionally, we have strengthened our partnership with DoD while building the National Background Investigations Services (NBIS) which will serve as NBIB's IT system to perform background investigations, as well as shared services for the end-to-end processes for all government agencies and departments. NBIB finalized its Business Process Reengineering Plan in FY2017 and formed a new Strategy and Business Transformation office that will address technology, process changes and data-based

Testimony of Charles S. Phalen, Jr.
Director
National Background Investigations Bureau
U.S. Office of Personnel Management
--
October 11, 2017

decisions to realize results in efficiency gains and to further support the development of NBIS. NBIB's work towards long-term solutions to reengineer processes and build out the requirements of NBIS has resulted in progress. As NBIS comes online, NBIB will be able to phase out our legacy systems in favor of NBIS.

NBIB conducted a comprehensive, interagency diagnostics assessment in FY2016 that identified 57 areas of improvement to address. Successes and progress thus far include the launch of a law enforcement liaison office and campaigns to improve quality of criminal checks conducted by all 23 investigative service providers (February 2017) and the release of the new national security questionnaire to be used by agencies (August 2017). Further, we are on-track to release eApplication (early 2018) and to release eAdjudication as a shared service to all agencies (fall 2017).

NBIB has developed strong interagency partnerships with the broader Security, Suitability, and Credentialing Line of Business community to identify and implement background investigation program improvements. As a member of this governance structure, NBIB engages with Performance Accountability Council Principals and DoD on a daily to weekly basis as the government's primary investigative service provider, and coordinates the 22 other delegated agencies that leverage NBIB's infrastructure in some capacity (e.g., electronic questionnaires, automated record checks, investigations, clearance repository, training materials, implementation policy guidance, etc.). NBIB has also continued engagement and provided solutions as part of an interagency initiative with the Presidentially-delegated Executive Agents (OPM and ODNI), OMB, and other stakeholders, including DoD, to reduce the investigation inventory more quickly. NBIB provided a substantial number of the ideas considered based on its vast expertise and ability to provide rich, historical data to inform decisions. Many of the efforts resulting from this idea sharing initiative are already underway by NBIB in close partnership with NBIB's 100-plus Federal customers and stakeholders.

NBIB is also supporting the evolving background investigation process by offering our customer agencies a continuous evaluation product in satisfaction of the guidance issued by the Director of National Intelligence in his role as the Security Executive Agent. NBIB will continue to expand coverage to fulfill future requirements and guidance issued by the Director of National Intelligence.

Our operations follow the investigative and adjudicative processes and standards set out by the Security Executive Agent. It is imperative this mission evolve by leveraging cutting edge technologies, utilizing shared services capabilities, and applying automation and innovative solutions to obtain rich and valid information in support of clearance determinations. It is equally

important that process improvements and methodologies are made across the entire enterprise in a standardized fashion so that quality investigative products facilitate the reciprocity of clearances across all government agencies and departments.

As we work to reduce the inventory, we will continue to explore new and innovative ways to meet our customer agencies' needs, leverage their expertise as part of our decision-making processes, and remain transparent and accountable to our stakeholders and Congress. We recognize that solutions to reduce the inventory and to maintain the strength of the background investigation program include people, resources, and technology, as well as partnerships with our stakeholder agencies and changes to the overall clearance investigation process.

Thank you for the opportunity to be here today, and I look forward to answering any questions you may have.

Mr. MEADOWS. [presiding.] Thank you.
Mr. Reid, you're recognized for 5 minutes.

STATEMENT OF GARRY P. REID

Mr. REID. Thank you, Mr. Chairman, members of the subcommittee. I appreciate the opportunity to participate in this hearing today.

I'll ask for the chair's indulgence on submitting a statement for the record as a late-add. We didn't get it over here prior to the hearing, but we will get it over here right away. Thank you.

To summarize my statement, the background investigation backlog is a matter of significant concern for the Department of Defense.

Long delays in obtaining security clearances are causing turmoil in personnel management, mission effectiveness, and technology development across the Department. This is within our military services, our civil workforce, and our cleared industry contractors.

Despite focused efforts to mitigate the backlog and the resultant negative effects on DOD, our senior leaders have called for new and innovative approaches to address issues of costs, performance, and timeliness within the personnel vetting enterprise.

As the committee is aware, Section 951 of the 2017 National Defense Authorization Act, required DOD to develop plans for assuming control of our background investigations, as is already done by 23 of their Federal agencies.

On August 25, Secretary Mattis approved the Section 951 plan and notified Congress, the Director of National Intelligence, the Director of the Office of Personnel Management, and the, Director of the Office of Management and Budget of his intent to look beyond the realm of incremental improvements and take full advantage of today's technology to alleviate the burdens of costly, time-intensive investigations that are hampering our mission-readiness.

The Department of Defense is well-postured to take these bold steps, and cognizant of the risks associated with such an endeavor.

In recent years, with the support of Congress, DOD has developed and tested new processes and capabilities for continuous evaluation and automated records checks to enhance, automate, and accelerate background investigations.

As of this month, the Department of Defense has 1.1 million personnel enrolled in a continuous evaluation program exceeding our annual goal. This program has demonstrated clear and compelling benefits of ongoing and more frequent vetting of cleared personnel.

These methods, which significantly decrease risks associated with periodic reinvestigations, have shown convincing results and provide the basis for new approaches to modernize the vetting enterprise.

Executing the Section 951 plan will provide DOD with the unique opportunity to build on our existing continuous evaluation and automated records checks architecture.

This work will be done hand in hand with the security and suitability executive agents, collaboratively developing alternative vetting procedures that ensure continued adherence to Federal standards.

We are ready to begin this process in early 2018, and incrementally shift new investigative casework to DOD and process them through approved, innovated architectures developed in collaboration with the executive agents.

By optimizing our investments and simplifying service delivery, we can achieve significant cost savings and cost avoidance, while, more effectively, driving system efficiency.

As we implement the Section 951 plan, we will remain committed to our task to design, build, and operate, secure and maintain the National Background Investigative Service NBIS that Mr. Phalen referred to. This is the single end-to-end IT, shared-service solution for all personnel vetting in the government, not only for NBIB, but for other Federal agencies that conduct background investigations.

DOD will remain committed to resourcing NBIB and NBIS throughout this transition process. I think that's an important point.

We would also continue to work very closely with the executive agents to streamline the legacy process, the process that exists today, to continue to identify ways to economize on field investigative work. We recently proposed and gained approval from colleagues here and in the Performance Accountability Council for a series of actions that are expected to produce near term reductions in the submission of investigative requests and reductions in field work.

We will continue to collaborate to identify these additional measures in parallel with our work to implement the Section 951 plan. And as a result of this work, NBIB will continue to process every case that DOD has already sent to NBIB from now and any point in the future. Once we stand up the 951 plan and develop alternative processes that are approved and vetted, we will route new work into that pipeline. This will take new work off of NBIB's plate, allow them to focus on the existing work as we continue to develop automated processes and feed them back into the overall architecture.

And, chairman, I would be happy to discuss the plan in more detail, and I look forward to your questions.

Thank you.

[Prepared statement of Mr. Reid follows:]

STATEMENT FOR THE RECORD OF

GARRY P. REID

DIRECTOR FOR DEFENSE INTELLIGENCE

(INTELLIGENCE & SECURITY)

DEPARTMENT OF DEFENSE

before the

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

on

SECURITY CLEARANCE INVESTIGATION CHALLENGES AND REFORMS

October 11, 2017

Chairman Meadows, Ranking Member Connolly, and Committee Members, thank you for the invitation to offer testimony on behalf of the Department of Defense on the status of personnel security clearance reform and the challenges that we continue to face.

The background investigation backlog is a matter of significant concern for the Department of Defense. Long delays in obtaining security clearances are causing turmoil in personnel management, mission effectiveness, and technology development across the department. This is within our military services, our civil workforce, and our cleared industry contractors.

Despite focused efforts to mitigate the backlog and the resultant negative effects on DOD, our senior leaders have called for new and innovative approaches to address issues of cost performance and timeliness within the personnel vetting enterprise.

As the committee is aware, section 951 of the 2017 National Defense Authorization Act require DOD to develop plans for assuming control of our background investigations, as is already done by 23 other federal agencies. On August 25th, Secretary Mattis approved the section 951 plan and notified Congress, the Director of National Intelligence, the Director of the Office of Personnel Management, and the Director of the Office of Management and Budget of his intent to look beyond the realm of incremental improvements and take full advantage of today's technology to alleviate the burdens of costly, time-intensive investigations that are hampering our mission readiness.

The Department of Defense is well postured to take these bold steps and cognizant of the risks associated with such an endeavor. In recent years, with the support of Congress, DOD has developed and tested new processes and capabilities for continuous evaluation and automated records checks to enhance, automate, and accelerate background investigations. As of this month, the Department of Defense has 1.1 million personnel enrolled in a continuous evaluation program, exceeding our annual goal. This program has demonstrated clear and compelling benefits of ongoing and more frequent vetting of cleared personnel. These methods, which significantly decrease risk associated with periodic reinvestigations, have shown convincing results and provide the basis for new approaches to modernize the vetting enterprise.

Executing the section 951 plan will provide DOD with a unique opportunity to build on our existing continuous evaluation and automated records checks architecture. This work will be done hand- in-hand with the security and suitability executive agents, collaboratively developing alternative vetting procedures that ensure continued adherence to federal standards.

We are ready to begin this process in early 2018 and incrementally shift new investigative casework to DOD and process them through approved, innovated architectures developed in collaboration with the executive agents. By optimizing our investigations and simplifying service delivery, we can achieve significant cost savings and cost avoidance, while more effectively driving system efficiency.

As we implement the section 951 plan, we will remain committed to our task to design, build, and operate secure and maintain the National Background Investigative Service, or NBIS. This is the single end-to-end IT shared service solution for all personnel vetting in the government, not only for NBIB, but for other federal agencies that conduct background investigations. DOD will remain committed to resourcing NBIB and NBIS throughout this transition process..

We will also continue to work very closely with the executive agents to streamline the legacy process, the process that exists today, to continue to identify ways to economize on field investigative work. We recently proposed and gained approval from colleagues here and in the Performance Accountability Council for a series of actions that are expected to produce near-term reductions in the submission of investigative requests and reductions in fieldwork. We will continue to collaborate to identify these additional measures in parallel with our work to implement the section 951 plan.

And as a result of this work, NBIB will continue to process every case that DOD has already sent to NBIB from now and until any point in the future. Once we stand up the 951 plan and develop alternative processes that are approved and vetted, we will route new work into that pipeline. This will take new work off of NBIB's plate, allow them to focus on the existing work, as we continue to develop automated processes and feed them back into the overall architecture.

Chairman, I'd be happy to discuss the plan in more detail. I look forward to your questions. Thank you.

Mr. MEADOWS. Thank you.
Mr. Evanina, you're recognized for 5 minutes.

STATEMENT OF WILLIAM R. EVANINA

Mr. EVANINA. Thank you, Chairman Meadows and members of the subcommittee. Thank you for the opportunity to be here in front of you today.

As the Director of the National Counterintelligence and Security Center, NCSC, I am responsible for leading and supporting the counterintelligence and security activities of the entire United States Government.

The Director of National Intelligence, DNI, is designated as a security executive agent. In this role,the DNI is responsible for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations, adjudications, and, as applicable, polygraphs for eligibility for access to classified information.

The NCSC has been designated as the lead support element to fulfill the DNI's security executive agency responsibilities. We're responsible for the oversight and policies governing the conduct of investigations and adjudications for approximately 4.1 million national security cleared personnel.

The security clearance process includes determining if an individual is suitable to receive a security clearance, conducting the background investigation, reviewing investigation results, determining if the individual is eligible for access to classified information, or to hold a sensitive position, facilitating reciprocity, and periodically reviewing continued eligibility.

We work closely with the agencies responsible for actually conducting the investigations and adjudications, and managing other security programs associated with clearances.

This ensures that our policies and practices are informed by those working to protect our personnel and sensitive information. In addition to supporting the DNI in its role as security executive agent, one of my other responsibilities is to support the DNI and the attorney generals' efforts to ensure that the departments and agencies across the Federal Government have Insider Threat Programs established to help deter, detect, and mitigate the actions of individuals who may have the intent to unlawfully disclose classified information, or possibly do harm to themselves or others.

The Insider Threat Programs go beyond traditional personal security practices implemented upon hiring, and offer an ongoing holistic approach to ensuring the well-being of the cleared workforce.

These programs help us to be more proactive in preventing unauthorized disclosures by minimizing potential security gaps and/or identifying personnel who need assistance in getting them help before any damage occurs.

The very first step in identifying and preventing an insider threat is the initial and periodic background investigation. This application and subsequent investigation, will continue with the clearance holder as the foundational assessment throughout the period of time the employee holds their security clearance.

So the interrelationship between the security clearance process and the insider threat detection is critical.

NCSC is engaged as a partner with NBIB and the Department of Defense in the transformation of the security clearance processes, and remains committed to providing departments and agencies policy direction, while continuously assessing new ways for improvement.

We have issued guidance to the community on a broad variety of topics, which are listed in my statement for the record.

Additionally, NCSC, in coordination with NBIB partners with Director of OPM, who serves as a suitability and credentialing executive agent to align the security clearance process for the national security, suitability, and credentialing. This collaboration has resulted in a number of achievements, which are also listed in my statement for the record.

We have also implemented efforts to track and report on the application of security clearance reciprocity.

Reciprocity, acceptance of background investigations and national security determinations support the employee mobility and mission accomplishment, which is a critical element to ensure maximum effectiveness in human resource utilization.

We are extensively engaged in modernizing security clearance processes, an effort that includes implementing continuous evaluation, to conduct automated record checks on a segment of covered individuals between the 5- and 10-year periodic reinvestigation cycles when security-relevant information may go unreported to security officials. CE is being implemented across the executive branch in phases.

In conclusion, Mr. Chairman, as holders of security clearances, we are custodians of our Nation's secrets, protecting the American people by protecting those secrets must be our highest priority.

I, along with my colleagues sitting beside me here today, are firmly committed to doing everything we can to address security clearance investigation challenges, and strengthen our Nation's security.

I look forward to your questions.

[Prepared statement of Mr. Evanina follows:]

**STATEMENT BY NCSC DIRECTOR WILLIAM EVANINA
FOR THE HOUSE COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT OPERATIONS HEARING ON
"SECURITY CLEARANCE INVESTIGATION CHALLENGES AND
REFORMS"**

Wednesday, 11 October 2017
Room 2154 Rayburn House Office Building
2:00 p.m.

Chairman Meadows, Ranking Member Connolly, and Committee Members, thank you for the opportunity to appear before you today to discuss security clearance investigation challenges and reforms.

As the Director of the National Counterintelligence and Security Center (NCSC), I am responsible for leading and supporting the counterintelligence and security activities of the U.S. Government, including the U.S. Intelligence Community.

The Director of National Intelligence (DNI) is designated as the Security Executive Agent (SecEA). In this role, the DNI is responsible for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations, national security eligibility adjudications, and, as applicable, polygraphs for eligibility for access to classified information. The NCSC has been designated as the lead staff support element to enable the fulfillment of the DNI's SecEA responsibilities.

We are responsible for the oversight of policies governing the conduct of investigations and adjudications for approximately 4.1 million national security cleared personnel. The security clearance process includes determining if an individual is suitable to receive a security clearance, conducting a background investigation, reviewing investigation results, determining if the individual is eligible for access to classified information or eligible to hold a sensitive position, facilitating reciprocity for these determinations, and periodically reviewing the individual's continued eligibility.

As NCSC exercises the SecEA responsibilities, it works closely with the agencies responsible for actually conducting the investigations and adjudications, and managing other security programs associated with clearances. This ensures

that our policies and practices are informed by those working to protect our personnel and sensitive information. One of those agencies is the National Background Investigations Bureau (NBIB); and its Director, Charlie Phalen, is also here today, along with Garry Reid, Director for Defense Intelligence (Intelligence and Security), Department of Defense.

I am going to focus my remarks on the efforts to improve security clearance processes and procedures, reciprocity, as well as the general challenges we face, including the backlog of investigations.

NCSC is engaged in a transformation of the security clearance process, and remains committed to providing Departments and Agencies policy direction, while continuously assessing new ways for improvement. We have issued guidance to the community on a wide variety of issues, which we would be happy to provide to the Committee.

Additionally, we partner with the Director, Office of Personnel Management (OPM), who serves as the Suitability and Credentialing Executive Agent, to align the security clearance process for National Security, Suitability and Credentialing. The following achievements have resulted from this collaboration:

- Creation of the National Training Standards for Background Investigators, National Security Adjudicators, and Suitability Adjudicators, which align training requirements across National Security, Suitability and Credentialing.

- Issuance of the Federal Investigative Standards (FIS), which align investigative requirements for suitability and national security, building upon previous investigative work, and avoiding duplication, where possible.

- Provided clarifying guidance to the position designation process using the Position Designation Tool. The tool aids in the classification of national security positions regardless of a requirement for access to classified information (i.e. Law Enforcement Officers). As a result, Title 5 Code of Federal Regulation (CFR) Part 732, was reissued as 5 CFR Part 1400.

We are extensively engaged in modernizing security clearance processes in an effort that includes implementing Continuous Evaluation (CE) to conduct automated records checks on a segment of covered individuals between the five- and ten-year periodic reinvestigation cycles when security-relevant information may go unreported to security officials. CE is being implemented across the Executive Branch in phases, due to the anticipated increased workload demands, technical complexities associated with developing personnel security enhancements, and the unknown impact to agency workforce requirements.

Initial CE implementation began in October 2016, with a requirement for agencies to begin conducting automated records checks on clearance holders and on those eligible to hold a sensitive position (such as a border patrol officers), by 30 September 2017.

Metrics collected during implementation will be evaluated to assess how we can leverage CE to transform periodic reinvestigations. NCSC is also building an IT system that will conduct automated records checks, apply standard personnel security business rules, and generate alerts when security-relevant information is identified. Our goal is to deploy a fully operational CE System by Fall 2018 that will be available for use by any Executive Branch agency.

NCSC is implementing the requirements directed by Congress in the Fiscal Year 2016 Omnibus Appropriation H.R. 2029 - 673 Enhanced Personnel Security Program (EPSP). The EPSP requires the DNI to direct Department and Agency heads to implement a program to provide an enhanced security review of covered individuals. No later than Fiscal Year 2021, the heads of the Agencies shall conduct automated records checks and check information from sources no less than two times every five years on the entire covered population, to ensure continued eligibility of each covered individual to access classified information and to hold a sensitive position. In response to the requirements of the Enhanced Personnel Security Program, we are working to incorporate capabilities developed through Continuous Evaluation to satisfy the requirement to periodically conduct records checks on all covered individuals.

As directed by Congress, the DNI, in coordination with interagency participation, will determine the feasibility of including additional data sources such as government, publicly available and commercial data, consumer reporting agencies, social media, and other sources.

NCSC is also finalizing a plan to assist in the elimination of the backlog of periodic reinvestigations. The periodic reinvestigation backlog elimination effort uses a phased approach and specifically identifies NBIB's need to expand production capacity, implement process improvements, and stand up a modernized and secure IT architecture to eliminate its internal backlog of investigations.

More broadly, NCSC is leading cross-governmental efforts to develop and implement improved investigative methodologies and processes to gain both short- and long-term advantages in managing investigative inventories and improving the quality and efficiency of the mission space. We interact at least weekly with partners at DoD, NBIB and other agencies to advance these goals and to ensure that as we move forward, we do so as a Federal enterprise in a manner which addresses the equities of all Departments and Agencies.

Mr. Chairman, I defer to my colleague from NBIB to provide perspective on specific background investigation issues and challenges. I look forward to your questions.

Mr. MEADOWS. Thank you, Mr. Evanina. Is that better than the first time?

All right. Mr. Hodgkins.

STATEMENT OF A.R. "TREY" HODGKINS

Mr. HODGKINS. Thank you, Mr. Chairman, and members of the subcommittee.

On behalf of the members of the Information Technology Alliance For Public Sector, I am pleased for the opportunity to share industry perspectives on the security clearance process in its current state.

I have to start by saying, I sadly feel like a character in the movie, Groundhog Day. In the mid-2000's, I testified several times before Congress, representing industry in what was then described as a clearance process. It was outdated and it needed modernization that addressed the backlog that rivaled the size of today's. It is a testament to how little has really changed.

The member companies of ITAPS appreciates the attention this committee is giving the issue. Like other sectors of the industrial base, the Information Technology Sector relies heavily on cleared personnel to provide IT goods, services, and solutions to the government mission.

Unfortunately, the process we use today to grant and maintain clearances continues to be outdated, and sorely in need of modernization, just as it was over a decade ago.

This is in addition to addressing the short term issue of backlog of investigations now numbering over 700,000. To put that into perspective, that's about the same number of people you represent in your congressional district, Congressman.

Industry outlined then what we believe was the path forward to modernize the clearance process, reduce the opportunity for another backlog to appear, and establish a 21st century process to protect the interest of the United States.

These criteria were known as the four 1's, and included one application, one investigation, one adjudication, and one clearance.

After meeting with stakeholders for almost a year now, we believe that these criteria still fit today's situation, and these steps should be used to guide efforts to address the existing problems in the system.

One application speaks to one singular digital form online that serves as a basis for a permanent digital security record for a clearance holder.

One investigation speaks to standardized investigation metrics and criteria to yield consistent, understandable findings that can be used across the government enterprise.

It also speaks to establishing real-time, continuous monitoring as the baseline for tracking clearance holders and as a replacement for reinvestigations.

One adjudication speaks to a dependable and repeatable set of standards by which agencies can determine whether an individual is eligible and suitable to be granted the privilege of a clearance, and for which a determination can be clearly understood across the government enterprise.

Finally, one clearance speaks to a dynamic where an applicant only applies one time for a clearance, is continuously monitored after it has been granted, and the clearance is accessible and transferable government-wide. It would also allow for industry personnel to move from one contract to another in a reciprocal fashion, all without having to undergo additional redundant examination.

These criteria outline a reform process that will deliver and enhance security on a real-time basis, while achieving maximum efficiency across the Federal Government.

Further, we believe that the reformation of the clearance process should not just look to catch up and draw down the existing backlog, but leverage technological advances to create a new dynamic needs of permitting access to our Nation's most important information, while securing that information from the threats it faces.

These technologies includes the application of big data analytics to the existing and past data set of clearance holders, to reveal patterns or anomalies that can lead to the discovery of insider threats, applying blockchain technology, to secure information and enable trusted information exchange, and the use of artificial intelligence to monitor trusted user activity and build trusted profiles.

Finally, industry has consistently supported the concept of a singular standardized clearance investigation across the government enterprise, and would oppose efforts like Section 938 of the Senate National Defense Authorization Act, to bifurcate the process.

Such an action would exacerbate, rather than relieve, the existing backlog, and enable agencies to silo their behavior regarding how they adjudicate and reciprocally treat clearances.

Section 938 would also force the government to compete against itself, and artificially inflate costs for the most scarcest resource in the process: the investigators.

Thank you again for the opportunity to share perspectives on the state of investigations for clearances and how we should resolve and evolve these issues. We look forward to working with you to reform and modernize the security process, and I look forward to answering your questions.

[Prepared statement of Mr. Hodgkins follows:]

Testimony of

A.R. "Trey" Hodgkins, III

Senior Vice President
IT Alliance for Public Sector

before a hearing of the

Subcommittee on Government Operations

of the

U.S. House of Representatives
Committee on Oversight and Government Reform

Wednesday, October 11, 2017

Introduction

Chairman Meadows and Ranking Member Connolly, thank you for the opportunity to share industry perspectives on the challenges industry and the federal government face in regard to the broken security clearance process. We applaud and encourage your oversight of the process and would hope that your attention will drive reform and modernization to the very serious threat the current state of the security clearance process poses.

The 21st century has brought new and ever evolving threats to our national and homeland security from inside and outside of our government and beyond the borders of our nation. Government agencies and departments have increased their reliance on private sector partners to contribute to the diverse national and homeland security missions. Unfortunately, the security clearance process has not adapted or sufficiently modernized to meet these demands and enable the government and industry workforce it takes to meet these new mission imperatives.

While the backlog of clearance applications is a major cause for convening this hearing, we hope that Congressional attention does not get lost on this recurring short-term symptom of a larger systemic problem. We recognize that as your partners in the federal contractor community, we do not hold a monopoly on the pain inflicted by the current system. The backlog impacts the ability of the federal government to investigate applicants and determine their suitability for employment, just as much as it impacts the ability for contractor personnel to get a clearance to work on a contract. We believe that holistic, government-wide security clearance reform should be the objective, as it is imperative to both security and productivity. As we move to reform the process, industry remains agnostic as to who "owns" the security clearance process; we are, however, resolute that any bifurcation to the process would only cause greater wait times, inefficiencies, waste taxpayer dollars, potentially create greater vulnerabilities, and undermine achieving a truly reformed clearance process.

A Brief History Lesson

The current predicament is not new. There are decades of reports from the Government Accountability Office detailing the challenges with the security clearance process and the backlog of applications. We must also recall that the security clearance process has been bifurcated in the past, with the Department of Defense (DOD) owning the investigative portion for DOD applicants as recently as the latter part of the last century. In fact, it was the inability of the Department to effectively manage the volume of investigations in that era that led to the consolidation of most of the government clearance and personnel investigative functions at the Office of Personnel Management (OPM). It was also the inability of OPM to effectively absorb that existing DOD backlog into a consolidated process that created the backlog problems of the early 2000s. We have seen these challenges before and recommend that Congress act now to not only address the short-term symptoms of the latest backlog of applicants, but also to invest in a permanent effort to address the systemic challenges of the security clearance process.

Executive Summary

The current the backlog of clearances awaiting investigation sits at over 700,000, a number that is unacceptable by any metric. Unfortunately, the immediate crisis that backlog creates is only part of the problem, as it injects increased risk into an outdated system that does not leverage the digital era to create a more effective security environment and which continues to inefficiently spend taxpayer dollars.

In the early 2000s, I worked with a coalition of industry trade associations who partnered with government stakeholders to identify the problems with the security clearance process that time, implement a long-term solution to resolve the situation, and create a pathway of process reform, modernization, and improvement. The situation improved in the wake of aggressive Congressional oversight by this Committee and others, culminating in the security clearance process reforms of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Unfortunately, the departure from that pathway of reform and modernization has contributed to the current state of security clearance processing.

Because we have gone back to the future with our current state, resulting in exorbitant wait times, ballooning costs, and systemic inefficiencies, ITAPS has re-convened the broad and diverse industry coalition to help assess the problems, and to suggest short and long-term solutions. In conjunction with our partners at the Aerospace Industries Association, the Association of General Contractors, the National Defense Industrial Association, the Professional Services Council, and the U.S. Chamber of Commerce, we have met and spoken with government stakeholders over the course of the past year. These stakeholders include the House and Senate Armed Services Committees (HASC/SASC), the House Permanent Select Committee on Intelligence (HPSCI), the Senate Homeland Security and Governmental Affairs Committee (HSGAC), the House Oversight and Government Reform Committee (HOGR), the National Background Investigation Bureau (NBIB), the Defense Security Services (DSS), the Office of Undersecretary of Defense for Intelligence (USD(I)), the Performance Accountability Council Project Management Office (PAC/PMO), and the Information Security Oversight Office (ISOO) at the National Archives.

At the time of the reforms of the IRTPA, industry brought forward a set of criteria to help guide the development of proposals and solutions to resolve the challenges the security clearance process faced. After our extensive engagement with stakeholders to assess the challenges we face today, we would submit to this Committee and others that those suggestions and criteria are still applicable and deserve resurrection to guide efforts to reform, modernize and improve the security clearance granting process today. We identify these suggestions as "The Four Ones":

- One application
- One investigation
- One adjudication
- One clearance

We have also advanced technologically and there are several options that can be applied to the process to improve efficiency, establish real-time monitoring of clearance holders, and better enable the counterintelligence mission to take stock of those trusted by the government. My recommendations and testimony will outline what each of these means, why we believe these criteria for reform still hold merit in today's situation and discuss the technological capabilities that can be applied at each step to enhance and improve the process.

Sadly, because these criteria still have merit today, it is a clear indicator of just how little has actually been improved in the clearance granting and maintenance processes. Adopting the Four Ones and the technological options will lead to a common operating picture, which we believe is the necessary end state for resolving the current challenges and positioning the process where it is ready for the threats and challenges of the new century.

Following the hack of OPM, on October 1, 2016, the NBIB was created to absorb OPM's Federal Investigative Services (FIS) and enable a centralized security clearance process. The FY 2017 National Defense Authorization Act (NDAA) required a report[1] from the Secretary of Defense (SECDEF), that was due on August 1st, 2017, detailing how the Department of Defense would move the investigation of DOD clearance applicants to the Defense Security Service (DSS), and on October 1, 2017, a plan was due from SECDEF and OPM on how to transfer these authorities. With barely more than a year passed since the creation of NBIB, a plan has already been developed to bifurcate the clearance process. Industry is concerned that such a bifurcation will undoubtedly lead to further and compounding inefficiencies. Additionally, this plan moved forward so quickly that DSS published an RFI on FedBizOpps.gov[2] on September 20, 2017, requesting: "market research to gather data for the purpose of developing requirements to contract for investigative service providers to conduct background investigations on Department of Defense (DOD)-affiliated personnel." The conflation of the reporting timelines, along with the issuance of the RFI, show that this process is anything but collaborative and measured and is not taking into account the detrimental effects it will create on the clearance granting process government-wide.

The Senate Armed Services Committee (SASC) included a provision, Section 938, in their FY 2018 National Defense Authorization Act (NDAA), S. 1519, that would move DOD clearances and the process surrounding them, back to the Department. The SASC recognized that something must be done to resolve this latest bout of problems with the security clearance system. We must oppose Section 938, however, because it does not adhere to the criteria of the Four Ones and will create a parallel process and duplicative regime in the Department that will increase costs and drain resources, cause further delays, hinder process improvements, and undermine efforts to move the government toward true reciprocity across all departments and agencies.

Despite prescriptive actions by Congress to address this systemic and enduring issue, problems persist. It will take Congressional oversight, Executive enforcement, and agency/department leadership to see meaningful changes implemented in the security clearance process. Finally, we hope to work with you to address the security clearance problem in a holistic, government-wide fashion. If the government seeks to deliver a more efficient, thorough, and secure process, it must include end-to-end digitization, shared services, utilize continuous evaluation, and leverage private sector partners for success.

Background

In order to perform many critical services for government customers, hundreds of thousands of industry personnel must obtain and renew security clearances every year. The security clearance process, rules, and regulations are very important to industry because they create the mechanism to obtain and clear qualified personnel to support the government's critical missions. Our suggestions, however, are not solely designed with industry goals in mind. Instead, our recommendations take a "whole of government" approach designed to create a system and processes that enable greater national security. Indeed, government employees, the priority in the security clearance process, are sure to benefit. We humbly recognize that national security is an inherently governmental function. Yet, it is the industrial base that provides critical capabilities to the government that enables mission success.

[1] Section 951, FY 2017 NDAA

[2] https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=38f74a6d1e492540bf7aed8d470efdd8

Industry faces increased pressure to deliver cleared personnel on the day a contract begins. The current state of the clearance granting process makes it almost impossible for industry to meet these demands. These delays in obtaining security clearances result in increased costs to the federal government, and ultimately the taxpayer, by delaying the ability to use the most qualified personnel on critical programs. In fact, industry has turned to "poaching" already cleared personnel to deliver contract needs. This process unnecessarily inflates costs of contracts and is the reality of a broken system. These costs run into the hundreds of millions of dollars for both government and industry. It also stifles innovation and cooperation, since it is virtually impossible to share a good idea or leverage an existing team to provide solutions across agencies or departments without having appropriately cleared personnel. Ultimately, we can only conclude that a considerable amount of important work is not getting done.

In the wake of the OPM breach of cleared personnel data, there was a contract to provide credit monitoring and restoration services for each person known to have had their records stolen. To pay for this contract, OPM apportioned the costs across their customer base. Many agencies, like DOD, lacked sufficient funding to both pay for new investigations and cover their portion of the contract, so the funds were used to pay for the service. Only when additional funding was identified were the agencies able to restore submission of applications for investigation. However, the ability to find an adequate number of qualified investigators to meet the investigation demand signal still perplexes the government. Bifurcating that process would only make that problem worse, while increasing costs.

One Application

"One application" envisions that an applicant would complete one standardized and digitized application that would become the permanent digital record and security history for an applicant and, if deemed suitable, a clearance holder. The "one application" goal made progress with the implementation of the e-QIP application format. NBIB is also rolling out in the near-term an updated, digitized Standard Form 86 (SF86). Standardization across the application process, however, is still lacking.

Also submitted with the digital application are fingerprints and signatures, which form the completed application package. Any one of these elements, if not submitted concurrently, can expire and delay initiation of an investigation, so coordination on submission is critical. In the effort to technologically enable the application process, the efforts to digitize fingerprinting is an area to be commended as, per NBIB, 94% of fingerprint collection is now done electronically. The next step in the process needs to be a digital signature and digital transmission, to a centralized database.

From this continuously accessible, digitized central repository comes the beginning of the total security history of an individual. As other elements of the Four Ones noted below, like continuous evaluation, become the norm in the national security process, we must enable the evaluation component from the beginning. Today, investigators are only given a static snapshot with which to judge a dynamic environment and dynamic individual. In the current process, such examinations only happen during the initial application and investigation, and thereafter only at 5-or 10-year intervals depending on the level of the clearance. We must also examine other elements that form the individual record, like foreign contact disclosure reports and other addendums, which are still handwritten, and move toward complete digitization of the forms and electronic submissions to the same repository to be appended to the total security history. Moving toward "One Application" would therefore enable dynamic access to the security history of a cleared person. Technology can enable all of these capabilities now.

One Investigation

One Investigation is vital to the continuity of the security clearance process and critical to the ability to achieve One Clearance, discussed later in my testimony. Unfortunately, agencies have historically disregarded investigations conducted on an individual and initiated a new process, even though the individual has already been investigated and has been granted a clearance. While this practice was statutorily prohibited in the IRTPA, it has not stopped agencies from refusing to accept the investigative conclusions of other agencies and many take the liberty to execute additional scrutiny of an individual. Many in government and industry are very familiar with the situation where personnel carry a multitude of different badges, each representing another examination.

Congress should examine this practice and determine if additional legislative prohibitions are necessary. At the very least, these re-examinations cause further delay in the overall effort to get cleared personnel on contract or in a mission area, and they can be a redundant, wasteful use of taxpayer funding. Congress should require uniform, government-wide standardization of the investigative process, protocols, and vocabulary employed to achieve One Investigation. Such an outcome would produce an investigative record that can be reviewed and interpreted consistently across government.

Technology also allows us to move beyond the static investigations of today because security situations are dynamic, and so, too, should be the investigations. In order to create a dynamic security situation, we should move toward continuous real-time evaluation of all clearance holders. One investigation becomes not only the initial investigation of an individual, but also a continuous analysis of public and private data sets for indicators and anomalies related to clearance holders. Continuous evaluation would also obviate the need for periodic reinvestigations at the 5-year (Top Secret) and 10-year (Secret) intervals.

Periodic reinvestigations (PR) are another key component in the clearance granting process badly in need of attention. In order to slow down the volume of investigations and avoid increasing the backlog at NBIB, agencies have taken extraordinary measures to extend clearance viability beyond the time requirements for PRs. Reinvestigations have been relegated to such a low priority that clearances held by industry personnel working on government projects sometimes expire before any action is taken to complete the renewal application. The condition is such that many periodic reinvestigations are considered to be "in process" once the clearance holder has completed an application for reinvestigation. In reality, many such applications are never entered into the process because the emphasis is placed upon those who do not have clearances, under the assumption that those with a clearance can be placed in a lower priority and be processed at a later date.

For government, this may seem to be an acceptable temporary solution. In practice, industry finds that more and more frequently, clearances have lapsed. These discoveries are made when cleared personnel try to move from contract to contract, start supporting a new agency under an existing contract, or relocate or get new employment and the validity of their clearance must be checked. It is at this time that both the employer and the clearance holder frequently first discover that, despite the completion of the periodic reinvestigation application, the paperwork was never processed and the clearance is "out of scope." Therefore, current clearance holders are now at even greater risk of having their clearance expire and/or lose their SCI access.

If we migrated to a One Investigation dynamic that included continuous evaluation, we can watch for the appearance of any "flags" or indicators (e.g. multiple foreign trips, foreign disclosures, divorce, financial

trouble, sudden financial gain, social media activity) that would show the need to reinvestigate an individual. In a situation where a cleared individual receives a clearance, and the very next day all these flags populate in an automated system, it would be pertinent and proper to investigate these occurrences rather than waiting 5 (TS) or 10 (S) years to delve into these issues. The consumer analogy is the real-time monitoring of credit by financial institutions. Charges to credit cards that appear fraudulent are immediately alerted to the consumer. This "real-time" condition should become the expected standard of investigation and evaluation of anyone with a clearance. But, reinvestigations are prescriptive on an arbitrarily determined timeline. In order to assess the status of this condition, industry would recommend that a survey of the backlog be conducted to determine exactly how many of the overdue applications are still valid, what steps be taken to ensure that cleared personnel are effectively scrutinized as appropriate, and that the clearances of industry personnel are not placed in jeopardy of being "out-of-scope."

One Adjudication

Industry has long sought standardization and uniformity in the process of adjudication and suitability determinations so that a person holding a secret or top-secret clearance could be confident that there would not be variances in the interpretation of their adjudication from one agency to the next. A uniform, government-wide adjudication standard will allow private-sector partners to rapidly execute on contracts. We recognize that suitability determinations may be different for the various level of sensitive work conducted within the government. A modular, building block type of suitability system, however, that even the least sensitive positions are investigated the same as the most sensitive, will produce common data and process. This will not only enable uniform insider threat data, but it will allow government and private sector employees to move from one department or agency to another with relative ease.

As one contract with an agency or department concludes, the need to move personnel to other contracts exists industry-wide. There is no salient argument for different adjudication standards across various government agencies and departments. The condition, however, is not limited to just the private sector. Federated U.S. government entities, such as DOJ and DHS, with multiple component agencies frequently do not acknowledge clearances issued within the same department. The concept of "one adjudication" builds upon the uniformity and standardization discussed above and leads directly into the following stage – one clearance.

To be commended, at this point in time, adjudication is the least problematic step in the process for industry. Once the investigation stage has been completed, the investigation record is returned to the requesting agency that is responsible for making the determination about suitability and eligibility and issuing the clearance. The most rapid portion of the security clearance has been, and continues to be, adjudication. Yet, even adjudication can be improved upon by standardizing the process.

One Clearance

Cleared professionals access much of the same systems, Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS), across government, so that all-source intelligence can help inform a common operating picture. Clearances, however, are not treated in the same manner.

One reason for the persistence of the conditions outlined in this paper is the lack of a single, government-wide, interoperable, real-time database containing all clearance and access information. The database

containing this information for the intelligence community, Scattered Castles, is classified and not linked to the same unclassified but sensitive database for the civilian and defense agencies- the Joint Personnel Adjudication Systems (JPAS) - which is slated to be replaced by Defense Information System for Security (DISS). There are also defense and civilian agencies that do not contribute information to the databases in a timely manner, making the clearance information issued by them incomplete or unreliable. Another hurdle to overcome is the requirement by some agencies to only recognize up-to-date clearances, (i.e., based upon a current investigation), even though the delays discussed above are pushing "active" clearances beyond their standard periodic reinvestigation timeframes. These requirements must be corrected for reciprocity to work as Congress envisioned it.

We have seen some improvement in the reciprocity of clearances, particularly in the intelligence community[3] with 86 percent reciprocity government-wide but instances when agencies refuse to recognize each other's clearances still occur with regularity. Another improvement industry has noted is the reduction in cases requiring a re-investigation of a current clearance by a second or third agency. Other onerous requirements short of a re-investigation, however, are still sometimes imposed and they serve only to slow down the process, duplicate efforts, increase the burden on taxpayers for redundant government activity, and prevent the agency from meeting its demands in a timelier fashion.

Ultimately, Congress and the Administration must require Federal agencies to provide accurate, timely, and thorough information about the clearances each has granted. This will enable the capability for others, when authorized, to review applications, the subsequent investigations, the results, and finally, the basis for adjudicating a clearance positively so that reciprocity can be fully realized wherever the national security needs of the United States demand.

Each agency has its own rules that prohibit smooth, timely movement of cleared contractor personnel from one contract to another. Despite prescriptive statues and guidance directing reciprocity, there is not reciprocity in practice.

The cost of doing business:

A systemic issue our coalition discovered was the cost of a security clearance is dynamic, versus fixed, throughout a fiscal year. DSS is reliably able to predict in a given year roughly how many investigations will occur. In doing so, expectations are established about the width of the investigation pipeline, which informs customers. However, between this prediction and execution, the cost of a clearance can and does change. This disparity leads to unfulfilled investigations due to budgeted versus actual investigations able to be executed in a fiscal year. Director Phalen of the NBIB has executed a fix to this issue, however, it is not in statute. We commend his leadership on this. We recommend that this change be codified so that future costs are known and able to be planned for, creating a measure of predictability and reliability in the security clearance process.

Conclusion:

Though this hearing was held to address security clearances in the present tense, we would be remiss not to point out future technology trends that will enable greater information and personnel security. Utilizing emerging technologies, like blockchain, to secure information and enable the trusted information

[3] https://federalnewsradio.com/workforce/2017/02/security-clearance-reciprocity-86-percent-governmentwide/

exchange among multiple parties through a shared ledger must be part of the conversation. Utilizing artificial intelligence to monitor trusted user activity, building usage profiles, and sharing it among all other agencies, will also create a roadmap to reducing risk. Finally, applying big data analytics to the data on all past and current clearance holders can help identify and develop better counterintelligence means to address threats. Siloed department and agency efforts to eliminate the insider threat problem only harms the greater good. This problem is not unique to any agency or department and the government must tackle the issue holistically.

Systemic issues still exist, enabled by arcane, bureaucratic red-tape, that promote distrust, slow favorable outcomes, and increase cost to the American taxpayer. Despite repeated prescriptive measures by multiple Congressional committees, the security clearance issues persist. From backlogs of 600,000 in 1999[4], to a low point in the first decade of the 21st century, and now 700,000, the cycle must stop by enacting true reforms.

In a "whole of government" approach, a singular authority must own the entire security clearance process – for security and accountability's sake. In this no-fail mission, a singular entity should standardize all processes and reign in the disparate systems and procedures that exist today. As security clearances are no more than a combination of a continuous counterintelligence investigation and operational security, it is incumbent to standardize and centralize the process with "The Four Ones".

It cannot be overstated that industry is committed to preserving the strict government requirements to obtain security clearances. The process, however, must be optimized to include leveraging industry relationships and deploying technology across the process. The interest is not to minimize current requirements, but to make appropriate changes to an antiquated process. This would allow the nation to remain vigilant in determining who has access to sensitive information while better meeting defense and intelligence needs at the lowest possible cost. Industry looks forward to working with the government to examine and implement these and other recommendations, and stands ready to devote its experience and significant expertise with best practices to ensure that critical government programs do not go unexecuted for lack of available cleared personnel.

Thank you for the opportunity to share our perspectives with the Committee.

RECOMMENDATIONS FOR CONGRESS AND THE ADMINISTRATION

1. Reinvigorate previous efforts to create one electronic record across a continuous digital process for clearances.
2. Tap the expertise of leading technology companies to partner with the national security community to apply new technological solutions to rethink the entire clearance process.
    a. DIUx, DARPA, IARPA, and In-Q-Tel enable wonderful outcomes, it's time to unleash them and others, on this problem.
3. Ensure that the security clearance process – from application, to investigation, to adjudication, to re-investigation – is technologically enabled; do away with paper files and ensure that all systems are interoperable and can share data across platforms and agencies.
4. Codify NBIB authority to align fee-setting with fiscal years, instead of allowing the practice to occur after budgets are fixed.

[4] http://www.gao.gov/products/GAO/T-NSIAD-00-148

5. Move from the mindset of a security clearance "process" to that of continuous evaluation.
    a. Just like counterintelligence and operational security is a dynamic process, so too should the security clearances process.
6. Enable information from employers to be used as a part of the security clearance investigation (e.g. college transcripts, previous employment history, etc.).
7. Establish a singular system of record, utilized by all 16 intelligence agencies and corresponding departments, that verifies the existence of a security clearance, without the clearance needing to be "passed."

Mr. MEADOWS. Thank you all for your testimony.

The chair recognizes the gentleman from Iowa, Mr. Blum.

Mr. BLUM. Thank you, Chairman Meadows, and thank you to our panelists for being here today.

The chairman should not feel bad about mispronouncing anyone's name on the panel. Last week I chaired a hearing and the gentleman's name was Mr. Hakes, and my notes said "rhymes with cakes." So, of course, I addressed him as Mr. Cakes. So don't feel bad, Mr. Chairman.

Mr. MEADOWS. Thank you.

Mr. BLUM. We currently have a backlog of 704,000 investigations.

What is the goal? I'm a businessman. So I hope we have a plan. I would like to know what our goal is for that backlog and by when. Does anybody have that answer? Because I know accountability is not exactly our strong suit in the Federal Government, but the voters want accountability.

Mr. PHALEN. I appreciate that. Thank you, sir.

I'll take a first cut at this. There is a steady state inventory level that is about 180,000 cases, and that was where it was during the late 2007 through 2014 timeframe, before we lost investigative capacity. And within that inventory, we were able to complete investigations within the timeliness standards that are outlined in the IRTPA legislation.

Mr. BLUM. Why did we lose capacity?

Mr. PHALEN. I'm sorry? When or why?

Mr. BLUM. Why?

Mr. PHALEN. The Office of Personnel Management terminated its contractual relationship with USIS, which held about 60 percent of our investigative capacity as a contract company.

Mr. BLUM. They were circumventing the contractual rules, correct?

Mr. PHALEN. So I would——

Mr. BLUM. Is that correct?

Mr. PHALEN. I don't know precisely. I do—I

Mr. BLUM. USIS, correct? They were circumventing the rules, the contractual rules? So I'm glad to hear they were terminated. In fact, I'm surprised.

Mr. PHALEN. Yes, sir. The relationship was terminated with them, and it was done fairly abruptly, and the individuals who were working for them, most of them did not come back into the service with any other contractor. They left the business. And so, that was about a 60 percent loss in capacity in the space of just a handful of single-digit weeks, almost overnight. And it has taken to, now, to build up that capacity, contractually, and through Federal hires, to get to a number that begins to approximate where we were in the early fall of 2014, when that contract was terminated.

Mr. BLUM. So do we have a goal?

Mr. PHALEN. Goal in terms of?

Mr. BLUM. Goal of investigative backlog by a certain date, we want to be at a certain level?

Mr. PHALEN. I have an approximation. We are dependent upon certain changes in process. Two things will have an impact on our ability to bring this backlog down.

Number one is hiring investigative capacity beyond what we have today. And we have commitments from all four of our suppliers to continue building that capacity to the extent possible. And if they are able to meet the goals that they have set for us, it will take approximately 3 years or so to bring down that inventory number to a manageable level that we want, perhaps even a little longer. That's without any other intervention.

The second level of intervention that would make a significant difference in our inventory numbers and our ability to hit timeliness goals would be our ability to look within the population that is already cleared, what is today covered by periodic reinvestigations, and leverage the advantage we have with continuous evaluation and other programs that go by different names, but do the same thing that will allow us, perhaps, to focus periodic reinvestigations into something that is less periodic and more focused on individuals that need that level of scrutiny and rely on the continuous evaluation tools to give us early warning, give the agencies early warning of folks that are representing a graver threat and not wait until the 5-year mark to find this problem. And that would take inventory out of my organization and allow me to focus my assets and my resources on what is the most important step, that first one, which is a baseline development of a level of trust in an individual first entering the Federal service or into a classified.

Mr. BLUM. So 3 years to get to—would that be like 125,000?

Mr. PHALEN. 180,000 is our goal.

Mr. BLUM. 180,000.

Mr. PHALEN. And our other goal is to meet the guidelines or the standards of an IRTPA, which is 80 days to complete a top secret investigation, and 40 days to complete a secret investigation. And just for clarification, the 3 years is me being terribly optimistic. It could be an extra 1 or 2 years beyond that. But that's——

Mr. BLUM. The investigations have become much more labor intensive?

Mr. PHALEN. They have.

Mr. BLUM. Especially since the theft of classified intelligence by Edward Snowden?

Mr. PHALEN. Yes.

Mr. BLUM. Now someone to the investigation has to be face-to-face versus telephonically? Do you agree with that, or do you think that's an overreaction?

Mr. PHALEN. So actually, investigations have been required to be face-to-face, for the most part, since when I was doing investigations, if not earlier, back in the early 1980s. The default is to do it face to face.

And what we have done with some of our mitigation efforts working, again, with the security suitability executive agent and the Department of Defense, is look for those opportunities where we can use technology, whether it is a telephone, or something as secure, video teleconference, to get to people who are in areas that we can't otherwise get to very easily.

Mr. BLUM. Can we make it less labor intensive?

Mr. PHALEN. Exactly.

Mr. BLUM. Can we do that? Is that possible through the use of technology?

Mr. PHALEN. Yes, it is.

Mr. BLUM. And that's in our plan, I assume?

Mr. PHALEN. The telephonic changes we're doing today. We have been running pilots with the video teleconference, particularly getting into areas in combat zones and other inaccessible zones to get to military members and have that conversation with them where we can't get an investigator on the ground. And we've been doing that as a pilot now for probably 4 or 5 months. It's been very positive working with the Air Force, and they would like to go more mainstream with that.

Mr. BLUM. And in closing here, I would like to say, though it's caused you an issue, USIS, that contract being terminated, I'm glad to hear that, because, to me, that represents accountability. So thank you for your answers. And I yield back the time I do not have.

Mr. MEADOWS. I thank the gentleman. The chair notes the presence of our colleague, the gentleman from Illinois. Mr. Krishnamoorthi. You think your name is tough, I ask unanimous consent that he be fully allowed to participate in today's hearing. And without objection, so ordered. And so the chair recognizes the gentleman from Illinois.

Mr. KRISHNAMOORTHI. Thank you, Mr. Chairman.

Mr. Reid, on September 6, 2017, Daniel Payne, the Director of the Defense Security Services, made headlines when he spoke at the Intelligence and National Security summit.

This summit was hosted by the Armed Forces Communications and Electronics Association and the Intelligence and National Security Alliance.

Director Payne said this, and I quote, "On a weekly basis, I got murderers who have access to classified information. I have murderers, I have rapists, I have pedophiles, I have people involved in child porn. I have all these things at the interim clearance level, and I'm pulling their clearances on a weekly basis. This is the risk we are taking."

Mr. Reid, are you aware of these statements?

Mr. REID. Yes, Congressman.

Mr. KRISHNAMOORTHI. Do you agree with him that murderers, rapists, and pedophiles have been given security clearances in the past?

Mr. REID. Congressman, I've spoken, I work for Dan Payne every day in our jobs. And in the first instance, I would just submit that immediately after this excerpt was published, we talked about this in terms of the context of his remarks, and the most important point he was trying to make, respectfully, was the impact of interim clearances and the effects of the backlog.

There are numbers that we can associate with revoked interim clearances, and we can provide that. I'm not sure it's appropriate to articulate those publicly. They refer to different categories of behaviors that are flagged.

There is a volume of some 200,000 interim clearances that DSS authorize. And the Director can authorize interim clearances under certain conditions for industry contractors, about 200,000 a year.

Several dozen of those you can map to some of these behaviors he was describing, but I would just say, Congressman, again, the description was intended to be more figurative than literal in terms of murderers and rapists. There are categories of behaviors that are within the guidelines that flag clearances. And that is what Dan was referring to. And we can certainly provide the numbers.

Mr. KRISHNAMOORTHI. Okay. Well, to me, I mean, murder is murder, rape is rape. In response to these alarming reports, on October 5, our full committee ranking member, Elijah Cummings, sent a letter requesting documents about these allegations. Because of the urgency of this matter, he requested them by yesterday, but so far, we have not received anything. No documents, no briefing, no responses at all.

Why is that, Mr. Reid?

Mr. REID. It's my understanding, Congressman that the Department is pulling a response together, and I'll have to verify, when I get back, exactly where it is and when it's coming over. But I am fully aware they are developing the response requested from the chairman.

Mr. KRISHNAMOORTHI. We want to know when we can expect to receive this information, sir.

Mr. REID. All right, sir. I'll take that back to the building as soon as I get out of here and we'll track it down.

Mr. MEADOWS. Excuse me. If the gentleman will yield for just a second?

Mr. KRISHNAMOORTHI. Sure.

Mr. MEADOWS. I mean, he makes a valid point. If there was a deadline for yesterday, and we're talking about security clearance backlogs, and you're having a hard time responding to a simple request from the ranking member, at what point are we going to get a response. Do you have staff here with you today?

Mr. REID. Sir?

Mr. MEADOWS. Do you have staff here with you today?

Mr. REID. Do I have my staff here, sir?

Mr. MEADOWS. Do you have some staff here with you accompanying you here today?

Mr. REID. We have our legislative liaison, sir.

Mr. MEADOWS. Let them check while we're going through the interview process. I'm sure that we would love, both in a bipartisan manner, to have some kind of update on when he can expect it.

Mr. REID. Yes, sir.

Mr. MEADOWS. I'll yield back and I'll extend your time.

Mr. KRISHNAMOORTHI. Thank you. Thank you, Mr. Chairman. And I echo the chairman's sentiments. You know, we would, you know, respectfully request that these documents be provided within 48 hours at this point. It shouldn't take longer than that.

Do you understand my request?

Mr. REID. Understood, sir.

Mr. KRISHNAMOORTHI. What risk does this pose when you allow criminals with those different behaviors, like the ones Director Payne described, to have access to classified information, sir?

Mr. REID. I'm not sure if I understood the question. The suggestion is not that known criminals are granted clearances;the clearance-granting guidelines are consistent. The comment was aimed

at behaviors that occur once people are in the workforce, and they create certain violations and their clearances are revoked. It's not the other way around. It wasn't a comment that a murderer is granted a clearance. The comment is someone with a clearance exhibits a certain behavior that breaks the threshold that's allowable. And it could be of any category. It's not, you know, murder is not the only category. That's obviously a very powerful category. There are other behaviors when the guidelines that one's clearance will be suspended.

Mr. KRISHNAMOORTHI. Now, if there's a backlog in processing these people, and they have committed these behaviors and they have clearance, that poses a risk. So what kind of risk does that pose?

Mr. REID. Well, again, there is not a backlog in identifying behaviors that break the threshold and raising those up for adjudication as soon as they are discovered. That is, that is not the context of the backlog.

When we're referring to a backlog, we're talking about cases that are in an open investigation. Your commentary, Congressman, we're talking about people that are in the workforce, in this case, with an interim clearance, they exhibit a certain behavior, it raises a threshold as soon as it's reported. Those aren't backlogged.

Mr. KRISHNAMOORTHI. So somebody who has committed these behaviors could be on interim clearance, correct? It's not automatically revoked or anything like that. It goes through an adjudication?

Mr. REID. The revocation process is the same for everyone. If the behavior becomes known, when it becomes known, it is reported through the security managers and raised up for a decision. Again, there's different categories of behaviors, but they all get acted upon. That is not a phenomenon—the backlog phenomenon we're referring to is not associated with flagging of behaviors.

Mr. KRISHNAMOORTHI. Mr. Phalen, let me just turn to you for a moment. Do you have an estimate of how often the government relies on interim clearances as a result of the current backlog?

Mr. PHALEN. I have an estimate, based on information I've received from the Department of Defense. And I think Mr. Reid just mentioned, there's as many as 200,000 today in the Department of Defense that are carrying an interim clearance, which is, essentially, all the national level, and to the extent we can capture them, local name checks and other electronic information that we can capture; plus no indication of misbehavior on the application to start with. And that allows them to put him in an interim clearance status pending the complete outcome.

Mr. KRISHNAMOORTHI. Thank you.

Mr. MEADOWS. I thank the gentleman.

The chair recognizes himself for a series of questions. So, Mr. Phalen, would you say part of the reason why Mr. Reid is wanting to take over is because you have such an extraordinary large backlog in clearances.

Mr. PHALEN. I think the backlog in clearances has been a significant catalyst in people asking how to reexamine, how to rethink the process of doing clearances. And certainly——

Mr. MEADOWS. So what hope would you give Mr. Reid that you're going to get it fixed? Because if you're not—listen, I'm agnostic in this in terms of whether it's you or Mr. Reid, but I am not agnostic in terms of it being both.

Mr. PHALEN. No, I understand.

Mr. MEADOWS. And so at some point, we're going to have to get serious about the backlog. You know, Mr. Hodgkins says it was Groundhog Day all over again. And what I don't want is another hearing a year from now to find that the backlog is still at 700,000-plus. So what are you doing to alleviate Mr. Reid's concern?

Mr. PHALEN. So fair question. So, number one, assuming we are left to our own devices here to work off the backlog and to work for the future, is to build the capacity and work within today's guidelines to reduce the levels—-

Mr. MEADOWS. So why haven't you done that already?

Mr. PHALEN. We are working on that. We've increased——

Mr. MEADOWS. I understand it's a work in progress.

Mr. PHALEN. Right.

Mr. MEADOWS. But we're at 700,000.

Mr. PHALEN. Yes.

Mr. MEADOWS. So why have you not put that—I mean, how can you be more aggressive, I guess, may be a better way to phrase that on alleviating some of the concerns?

Mr. PHALEN. So continuing to grow that capacity, which, again, and we've seen from experience, that the growth in investigative capacity is the single biggest positive effect upon reducing the backlog and getting to timeliness.

The second piece is working very hard, and we've gone through two cycles of this now, in finding opportunities to reduce the level of effort that is required without compromising our virtues, but reducing the level of effort required to complete a clearance. And I would say, the third thing that we are beginning to work on, and this is a collective agreement amongst all of the principals, and I think one or two of the speakers already mentioned, is that we need to look at the future and fundamentally ask ourselves how do we do this differently?

Mr. MEADOWS. Well, but Mr. Hodgkins made the point, he said that you should have looked at that 10 years ago.

Mr. PHALEN. Sir, I wasn't in this role 10 years ago, but he's right. I would perhaps argue we should have look at this longer than 10 years ago. I have found evidence——

Mr. MEADOWS. So what you're saying is you're new to your role and you're taking this serious and you're going to make an effort to accommodate and make sure that Mr. Reid gets the security clearances that he needs?

Mr. PHALEN. The short answer is, that's exactly why I came back into the Federal service to do that task.

Mr. MEADOWS. All right. So Mr. Reid, let me come back, because I think there was a little bit of cross-talk between my colleague here to my right and what you were saying. He was talking about interim security clearance. You said that there was, what, 3 dozen? Several dozen? Several dozen?

Mr. REID. Of the 200,000 interims that were granted by DSS in 2017, there were some number—I don't have it—I can look it up

here, 100-plus or so that fell into the revocation status. And within those categories, single and some double-digit numbers that refer to sexual misconduct, criminal behavior, that's what I was trying to characterize to the Congressman.

Mr. MEADOWS. So, but on an interim basis, would not a normal background check have picked that up?

Mr. REID. Again, these are behaviors that are occurring after they are granted.

Mr. MEADOWS. Well, but the very definition of interim is that you're actually going into a setting where you're getting a security clearance. And so as we look at that interim basis, that's what I'm saying, your testimony and what he asked doesn't seem to be jiving. Because I've got several employees that are now working for the administration that are on interim security clearances. They left my employment and they went to work where they had to get a security clearance. Well, you would think at that particular point, when they get an interim, they would do a normal criminal background check. So did you do criminal background checks on all of those people?

Mr. REID. Everyone that is granted an interim is granted an interim only when they submit a request for a clearance. And as Mr. Phalen said, if their initial screen comes up with nothing derogatory, and I don't want to get technical, but if they meet the bar of no derog, they can be granted an interim clearance. And it depends on what job they're in. It's not uniform across even DOD——

Mr. MEADOWS. No, I get that.

Mr. REID. They're still—their investigation goes into the queue. And that investigation will run its course and come back final, once it's adjudicated. Within that time frame, if people misbehave——

Mr. MEADOWS. This isn't any first rodeo, I get that.

Mr. REID. Okay.

Mr. MEADOWS. I understand the process.

Mr. REID. I'm sorry, if I'm not understanding——

Mr. MEADOWS. What I'm saying is, is before you give them an interim clearance, do they pass just a normal criminal background check?

Mr. REID. An initial check, yes, sir.

Mr. MEADOWS. All right. So every one of those people that he had on the list, passed a criminal background check?

Is that your——

Mr. REID. Yes, sir. The initial checks. The initial layer of checks, with nothing derogatory, you may grant them an interim.

Mr. MEADOWS. All right. And so how do you find this? Was it when they got their security clearance?

Mr. REID. The behaviors occurred after they were granted clearance.

Mr. MEADOWS. So you had murderers and all of that after——

Mr. REID. The examples of misbehavior were in the context of Mr. Payne's comments, things that were occurring to people that had been granted——

Mr. MEADOWS. So they weren't missed in your interim clearance?

Mr. REID. Correct.

Mr. MEADOWS. Every one of them?

Mr. REID. Best of my knowledge, sir.

Mr. MEADOWS. All right. Well, that's why it's imperative that you get the kind of information to the ranking member that he requested. And so I assume—I'll give you just a second to turn around to your staff. Is somebody working on that to get us a response?

Mr. REID. Working on it, sir.

Mr. MEADOWS. All right. Very good.

So Mr. Reid, what makes you think that you can do it better than Mr. Phalen?

Mr. PHALEN. I appreciate that question, sir.

Mr. MEADOWS. This is softball. This is your chance to hit it out of the park.

Mr. REID. I appreciate it.

Mr. MEADOWS. And if you swing and miss, it's going to have consequences. So go ahead.

Mr. REID. Don't you know it. I appreciate it.

It's not 10 years ago. What's different now, and what's only in the last few years made available to us, is the ability to fuse multiple sets of data, data that have been put in place as a result of incidents, some of which were referred to, Navy Yard, Fort Hood shooting, Snowden, Manning.

We have a large enterprise within DOD for an Insider Threat Program. We have, at the component level, 43 subcomponents in the Department have Insider Threat monitoring programs.

We have a continuous evaluation program that I've been exercising on a slice of the Department of about 500,000. We're going to be at a million very quickly. We bring in data sets——

Mr. MEADOWS. So now is this the check that maintains the clearance that you're talking about it?

Mr. REID. The check that used to maintain the clearance, right, correct,

Mr. MEADOWS. This is not the initial one, this is actually on the maintenance?

Mr. REID. Well, it could be both. What we are professing——

Mr. MEADOWS. I understand what it could be. I'm asking what it is.

Mr. REID. Today we have used our continuous evaluation programs that we're conducting only on a sample basis to actually highlight behaviors that triggered revocations far in advance of when the next periodic review would have been. That's proven itself. Our continuous evaluation program, we ran pilots over the last several years. We took a completed investigation. We took a CE data set and said, "could you have done this investigation the same way using CE?" And we got over 95, 96 percent correlation of things that were found. So we've been proving——

Mr. MEADOWS. So do you have a technical background? So are you an IT guy?

Mr. REID. Me, sir? No, sir.

Mr. MEADOWS. Okay.

Mr. REID. We have IT guys.

Mr. MEADOWS. Do you know what blockchain is?

Mr. REID. I'm not 100 percent familiar with that term.

Mr. MEADOWS. All right. Mr. Phalen, let me skip before I let you finish off here. Because, you know, he's making some points, and so at what point would you disagree with that?

Mr. PHALEN. To the points he made, I do not disagree with.

Mr. MEADOWS. So you think that he should have that ability?

Mr. PHALEN. So I think he has that ability. He has that responsibility right now to conduct continuous evaluation.

Mr. MEADOWS. So if we took resources from you and gave it to him, are you saying that he could do a better job than you could?

Mr. PHALEN. No, sir, I'm not saying that.

Mr. MEADOWS. Okay. I just want to make sure. That was a softball to you.

Mr. PHALEN. Okay. I misunderstood the question, sir, I'm sorry. And I'm not sure if the Representative from Illinois is a Cubs fan or not.

Mr. MEADOWS. He is. You just—not a swing and a miss. You did good. Go ahead.

Mr. PHALEN. Okay. What I believe Mr. Reid is referring to is the use of continuous evaluation to monitor individuals near real time in the workplace. This is different than what is today's model, which is to use periodic reinvestigations at the 5- or 10-year level, which is something that is done externally by my organization.

I believe that much of that work can be supplanted by, after due consideration by much of the continuous evaluation that is required and being done within the Department of Defense, the intelligence community and a lot of cleared industry right now. And that that can be leveraged against the requirement to do periodic reinvestigations, and that those resources that are currently involved in periodic reinvestigations within my organization, or in any investigative organization, can be redirected towards the initial evaluations to work with those people who have not yet been cleared and focus our energies on that.

Mr. MEADOWS. Okay.

Mr. Evanina, I got a note here that said, I guess the rollout of the continuous monitoring program that was originally for, I guess, October of 2016, that you were going to roll it out in phases, or it was being rolled out in phases. I mean, what are the barriers to making sure that it goes government-wide?

Mr. EVANINA. Sir, that's a good question. None. We are completely on schedule with our CE program. And it's important to back up a sec and talk——

Mr. MEADOWS. Hold on. We may have news breaking here. You're saying there are no barriers and you're on schedule?

Mr. EVANINA. We are on schedule.

Mr. MEADOWS. That is, let me just applaud you, because that's probably one of the first times I've ever had in one of these hearings where I've gotten both "there are no barriers," and "we're on schedule." So kudos to you. Go ahead.

Mr. EVANINA. Thank you, sir. But it was not without pain,I'll grant you that, to get to where we are now. But I think we need to step back a little bit and talk about what continuous evaluation is. We decided a few years ago to split it up into government. And what DOD's continuous evaluation program has been successful at this point is germane to DOD. And what Mr. Phalen and BIB are

doing is germane to their processes. But we were doing at NCSC is providing a service to all executive branch agencies to opt into our continuous evaluation program to allow agencies to use our services for a couple reasons: Efficiencies of scale and cost, as well as provide agencies outside the intelligence community who don't have the ability to procure these services to have the opportunity to get them from us, whether they are one of the top seven or eight databases we check. So this is in all-of-government executive branch program that we're facilitating.

Mr. MEADOWS. Mr. Hodgkins, I'm going to ask you one question before I recognize the gentleman from Illinois for a second round of questions. So we talked a little bit, or you mentioned in your testimony blockchain. And for those of us that are not technically savvy, fortunately, I have a brother that can tell me about blockchains and the secure way that we can communicate and compartmentalize that. So as we look at that—other that blockchain, what are some of the other technology aspects that we could actually deploy, whether it is at DOD or OPM that would help streamline this?

Mr. HODGKINS. Well, the other suggestions I made in my testimony referred to artificial intelligence. So the——

Mr. MEADOWS. For most of us, that's a danger. We get concerned when we hear about artificial intelligence. It is kind of—well, I won't go there.

Mr. HODGKINS. The commercial analogy I can point to, sir, is the financial services and how they monitor your credit. And if there is behavior that appears to be fraudulent on an almost real-time basis, you're notified of that. They are asking you, is this you making this transaction, if you travel somewhere out of the ordinary.

Mr. MEADOWS. So why have we not deployed that today in this realm?

Mr. HODGKINS. Well, as the other panelists have identified, they are beginning to roll that out, but it is something that industry called for over 10 years ago, suggesting that that move to replace the periodic reinvestigation process eventually began as, I think Mr. Phalen noted, and Mr. Reid noted, that there are high degrees of compatibility, or alignment with the manual reinvestigation of an individual and using the automated processes and what they find, which has always been the question in using this capability. Do they find the same things? Will we still find the same bad actors, and identify them for the same reasons?

So it is heartening to hear that that is the direction they are moving and that they are making advances and there are no obstacles. But using those capabilities in the way the financial services market does for credit monitoring, for any individual, is an example we would point to, an analogy we would point to, about how this could be deployed to look at things like criminal histories, although those are poorly automated across the country, particularly at the State and local level. We can look at marital records; we can look at financial records; and then we can look at other databases that are out there, either commercially available or in the possession of the government.

And Mr. Evanina noted they are looking at several, and we can continue to identify and tie into and bring online additional data

sets that would reveal other flags about someone who holds a clearance, and we think we should continue to push out in that direction.

Mr. MEADOWS. All right. So the chair recognizes the gentleman from Illinois for a second round of questions.

Mr. KRISHNAMOORTHI. Thank you, Mr. Meadows.

Mr. Phalen, as the NBIB director, I don't think it is an exaggeration to say that you are a key player in our national defense and counterintelligence apparatus, making sure that the American people can trust secrets to remain secure is a vital task. Now, the security clearance process, as we all know, relies heavily on the proper completion of the standard form 86—SF–86 form. And as you know, complete valid and accurate answers to the questions on this form are vital for the security clearance process.

What does the NBIB, or any other background investigative agency, do to ensure that the information on an SF–86 form is accurate? You don't take applicants merely at their word, correct?

Mr. PHALEN. Generally not. Much of the process is to validate that the information on the form is correct, both in terms of locations they worked, locations they lived, their claims of either some or no criminal involvement. Essentially they are explaining their life on this form, and our goal is to go validate that they have been correct in that, and to seek other information where it appears that it may be incorrect.

Mr. KRISHNAMOORTHI. And, obviously, everybody makes mistakes. Let's say I made a mistake on the SF–86 form. I'd have a chance to correct it. Is that not right?

Mr. PHALEN. So in the subject interview when an investigator is speaking to applicant, going over the form, and talking to them about things, if there is a mistake to be made—that has been made, it can be corrected. And the agent will put that into the investigative report and that will be captured. What that mistake is may be dispositive of how much further we're going to dig. If it's something simple like the middle initial being wrong or I got the dates wrong in the years I was in high school, not a big deal. But if I forgot to mention a significant felony conviction, that would be far more substantive and we would want to go pursue that a lot further.

Mr. KRISHNAMOORTHI. Ah-ha. Forgive me, I'm new to government. I spent most of my career as a small businessman, so I'm going to ask you some really perhaps some simplistic questions in your world. But what if I were to make several errors with my SF–86 form, not just one, but a bunch? What would happen in that instance?

Mr. PHALEN. Again, it would depend on what kind of errors they were. One of the concerns we have had is in the current form the electronic SF–86, is to use technical talk, a little bit kludgy and can be prone to some level of people making mistakes, and so we take that into account. In fact, we are working together with other elements of the government to build an new electronic application form that is far more user friendly, and will lead to less errors on the front end, and even perhaps do some fact checking on behalf of the applicable doing it. To answer your question, if it was a number of errors, it would depend.

Mr. KRISHNAMOORTHI. I mean, how many do—what if there are errors, even in my correction, how many do-overs do I get?

Mr. PHALEN. Fair question. Ultimately, we would capture the information as much as we could capture from the applicant and try to verify it. At some point, we will make a decision to send the information to the adjudication facility that it makes the ultimate decision about whether an individual gets the clearance and let them judge for themselves as to whether they think this is too much or not too much.

Mr. KRISHNAMOORTHI. I understand. This isn't a hypothetical situation. As you know, senior White House advisor Jared Kushner submitted four addendums to his security clearance paperwork after his original SF–86 forms contained more than 100 errors and omissions. Mostly related to the failure to disclose foreign contacts. Retired General Flynn failed to disclose payments of over $600,000 for his work representing authoritarian regimes in Washington. Both were approved for their security clearances. What would you do if one of your employees approved such an incomplete form?

Mr. PHALEN. So I'd un—working in the hypothetical, without using any particular subjects on this, if the investigator did not—if the applicant said, I didn't do this or I never—or failed to report it, the question would be how does investigator find it was failed to be reported? And if the investigator discovered that it had been failed to be reported, the first step would be to go back and try to understand what—why it was missed and what was missed and capture it again. What I don't know in the particular cases you're talking about is we have no visibility in our organization to any of those activities. Those are done by other organizations, what that meant. But there would be a point when an adjudication facility, an adjudication organization, has to take into account those mistakes. It is not our decision to make that decision. It is not in our purview to make that decision. We simply report what we know and how many addendums there may be to a report, to report that.

Mr. KRISHNAMOORTHI. Is there ever an instance where someone can command you to fast-track the verification of an SF–86 form?

Mr. PHALEN. It depends how you define fast-track, sir.

Mr. KRISHNAMOORTHI. Cut corners, fast track, get it through, ram it through the system.

Mr. PHALEN. Cutting corners, no. So if people ask us to do things, to put things ahead of queue, yes, we do that all the time. To cut corners, we do not do that.

Mr. KRISHNAMOORTHI. Can you recall if there's ever been an application having to submit four addenda detailing over 100 errors and omissions being able to maintain their security clearance once those errors and omissions had been identified?

Mr. PHALEN. I will caveat that by saying I have not seen the breadth of all the applications, but I have never seen that level of mistakes.

Mr. KRISHNAMOORTHI. Neither have I. It's clear that there is a lot more ground to cover on this. Mr. Chairman, you are doing a great job here. I hope that you will convene further hearings on this subject, because it really bears investigation. Thank you, sir.

Mr. MEADOWS. I thank the gentleman from Illinois.

The chair recognizes himself for a series of follow-up questions. So Mr. Reid I interrupted you when you were making your closing remarks on why you would do such a fantastic job, so I will go ahead and let you finish.

Mr. REID. Thank you, Chairman. To continue, the DOD plan we talked earlier about goals, our plan is to alleviate the burden on the backlog in the near term by shifting that work into an alternative process, focusing on the secret level investigations. We submit about 700,000 investigative cases to NBIB every year, about two-thirds of those are at the secret level, initial or reinvestigation. Based on the strength of the continuous evaluation, automated records checked and the fusing of all these data sets that we have already built within the Department to monitor performance and behaviors and spot anomalies, we are prepared, as early, starting in January, to work with the executive agents to get approval to use these systems as systems of records to meet the performance requirements, the Federal standards required to approve a secret level clearance.

Doing that—so that process we'll start in January, we envision within a few months, having those approved. We turn off the spigot of new secret cases. Again, this is about 500,000 a year that go to NBIB. We will incrementally do this, alleviate the pressure valve on their system, allowing the capacity they already have to focus on the workload they already have and to prove this system as we build it. It's a phased process focusing initially on the secret.

More than 90 percent of NBIB secret cases are DOD. This is very much a DOD issue. Almost every servicemember—in fact, every servicemember is cleared at the secret level upon entry into the service. So we have a very high volume, and we feel like the risk—the risks associated with this, knowing that we have proved and piloted systems, it is worth taking the next step to take the pressure off.

Mr. MEADOWS. Tell me about the pilot.

Mr. REID. We ran pilots for several years in DOD.

Mr. MEADOWS. How many people?

Mr. REID. Total that we piloted actual cases on, it is in the hundreds of thousands. And we have enrolled——

Mr. MEADOWS. And you were able to complete those how quickly?

Mr. REID. We put the pilots in place, we ran them for periods of 6 months at a time. For instance, initially, we took a slice of people——

Mr. MEADOWS. So how much faster than Mr. Phalen is doing it?

Mr. REID. Well, they are not doing it at all presently but we are——

Mr. MEADOWS. Because—I would beg to differ on that particular thing. So how much faster than Mr. Phalen? Mr. Phalen, are you doing that?

Mr. PHALEN. So, I would probably need to clarify whether we are talking about initial investigations or periodic reinvestigations.

Mr. MEADOWS. I think we are talking periodic re——

Mr. REID. Initially, secret level periodic going within 2 years to initial secret.

Mr. MEADOWS. Right.

Mr. PHALEN. So currently we are running the same automated checks through our system, what we have to do under today's process.

Mr. MEADOWS. So you're shaking your head no. Is he not doing the same automated checks? You are both sworn testimony. So is—Mr. Phalen, are you doing those automated checks?

Mr. PHALEN. When you put their system and ours side by side, we are doing the same automated checks.

Mr. MEADOWS. Mr. Reid, you're shaking your head no.

Mr. REID. When we implement the DOD plan, which we want to start in January, the initial phase of that is to gain additional approvals. That's the part where I said what we are proposing to do isn't that same as what's being done today.

Mr. MEADOWS. So you pilot program—is he doing the same thing—in your pilot program, did he do the same thing?

Mr. REID. Today those things are being done based on the pilot.

Mr. MEADOWS. Yes or no, just tell me yes or no. In your pilot program is he doing the same thing that you did in your pilot program?

Mr. REID. Not to my knowledge.

Mr. MEADOWS. Mr. Evanina, is he doing the same thing?

Mr. EVANINA. Sir, I'm not sure of the fidelity of both programs to answer.

Mr. MEADOWS. Sure, I'm all ears.

Mr. REID. We are not using these systems now as systems of record to complete investigations, and neither, I believe, is NBIB. We have data available. We have employed methods of automated records, checking and seeing. We have not implemented those as a system that can grant, one, a completed investigation. That is the step that we want to take in——

Mr. MEADOWS. So how do you know that that will work?

Mr. REID. I'm sorry?

Mr. MEADOWS. How do you know that that will work?

Mr. REID. Because we have run the test and run the pilots. We feel——

Mr. MEADOWS. No. How much quicker are you doing things than OPM?

Mr. REID. We will implement this starting in January, within the first 12 months, we have a three-phase plan. By the end of the first phase, we believe we will reach a point where there will be no more secret reinvestigations, which is about 300,000 a year that will not go to NBIB, made the first year.

Mr. MEADOWS. A critical thing, you said "we believe." What quantitative data do you have to support your belief?

Mr. REID. The data would be based on the pilots, and the testing that we've done, and our confidence in our executive agents.

Mr. MEADOWS. Confidence is not quantitative.

Mr. REID. You're correct, sir. We have tested these systems, and we believe they are ready to be implemented. We have to work with the executive agents to gain their approval to implement them.

Mr. MEADOWS. Mr. Phalen?

Mr. REID. It will be done much faster.

Mr. MEADOWS. Mr. Phalen, do you agree with that? Can they do it better than you can do it? Here is the thing, is my problem, and actually it has been mentioned over here, moving something from one bucket of the government to another bucket of the government does not necessarily create more efficiency. It—generally, it does not. And so I am skeptical that we are going to get all these unbelievable efficiencies just by moving it from one government agency to another. And what we're going to do is end up with duplicative services, and I'm all about shared services, you can Google it and you can figure out where I am on that. I am all in. But what I'm not about is allowing DOD and OPM to do the same thing when, Mr. Phalen, you said that the basic problem that you have is getting talent to actually do these checks. Is that correct?

Mr. PHALEN. To do the checks that involve a human-on-human interaction, yes.

Mr. MEADOWS. So how are you going to fix that, Mr. Reid?

Mr. REID. The efficiency, sir, it is a three-part process. There is submission, investigations and adjudications.

Mr. MEADOWS. So would you submit that DOD is a model of efficiency?

Mr. REID. I'm suggesting that putting submissions, investigations and a adjudications under a single agency is inherently more efficient because of the ability——

Mr. MEADOWS. If that's your argument, then we would put it all under OPM.

Mr. REID. Well, sir, because the level of data that we intend to bring into this process resides within our components and there's data—monitoring data that is not readily exportable to be outsourcing the readiness of the Department of Defense. We have an opportunity because of the maturation of these programs, these insider threat and CE programs, this is the first opportunity we've have to bring all of this under an integrated architecture. And it's——

Mr. MEADOWS. So in your pilot, what did you figure out that you didn't do well?

Mr. REID. We—it was mentioned earlier, solely relying on electronic data sets, there are gaps in State and local law enforcement flags that, to the best of our piloting, we can't reach out into every county jurisdiction in real time and find out something happened last night. Okay?

So the next step is to continue to bring in all—as many sources as we can, and with the right algorithms and we are using our innovation offices to develop these processes, to see how far you can go before you have to actually get to somebody knocking on somebody's door. We've never proven that nobody ever needs to knock on anybody's door. But with the secret level of checks—the top secret is definitely harder, but at the secret level, we have enough experience in this to be prepared to recommend to the executive agents that it is a suitable alternative process to meet the intent of the Federal guidelines doing the checks to verify the veracity of the individual's application and the reliability of the individual, a large majority of that at the secret level initially.

We believe we can get further, but we're focused on secret up front. That's the largest piece of work we give them, that that data

is in the Department already, we don't think it's necessary to build a separate process to send it somewhere. We are building the entire end-to-end IT system, that was already the DOD task from the review that created NBIB. That is a DOD system. It is a DOD system with DOD data. The missing piece is our investigative responsibility relies there. But it is not a bifurcation. They do 100 agencies. There are 23 other agencies that do what we're asking to do.

Mr. MEADOWS. Mr. Phalen, I mean, Mr. Reid's making a compelling case. I mean how do you respond?

Mr. PHALEN. I respond on a couple of threads. I think we are in complete agreement. Where I would concur with what his statements are is that in the realm of the periodic reinvestigation, there is information within each agency that has responsibility for the folks in that agency that are cleared, whether staff or contractor. They all have information that generally is not available to our investigators when they are doing——

Mr. MEADOWS. So you're saying that they are better suited to do that?

Mr. PHALEN. I think any agency is better suited to work on those and people that are already inside the organization. They will have a better optic——

Mr. MEADOWS. So what are they not better suited at?

Mr. PHALEN. I defer whether it is better suited or not better suited, but for——

Mr. MEADOWS. No. I'm asking you for your opinion. I mean, Mr. Reid gave me his opinion very clearly. If not, you're going to have a missed opportunity here. I want to have your opinion.

Mr. PHALEN. We have both an electronic and a geographic reach that is across this country, and for any initial investigation at whatever level, tier one through tier five, we have the ability to reach out, real or near real time, to find information. They don't have that capacity today.

Mr. MEADOWS. How would you get that, Mr. Reid?

Mr. REID. We have 43—40-something field offices under the Defense Security Service in the United States, we have combatant commands in investigative capacities stationed all over the world.

Mr. MEADOWS. But that doesn't make you efficient.

Mr. REID. No. But that's how we would cover the same ground. We have field offices, others have field offices, we have a robust——

Mr. MEADOWS. So Mr. Phalen, I may have misunderstood you. Is it your presence that allows you to do that, that you have multiple locations, because that's what Mr. Reid is saying. I didn't think that's what you were referring to.

Mr. PHALEN. So it is both electronic presence where we can get information electronically, and it is physical presence at 86 field offices around the country, and folks stationed at overseas locations to do this work. And that's what allows us to get the local records, and to what is a key piece, particularly to a periodic reinvestigation as it exists today within the process and any initial investigation, that there is a human-to-human interaction at wherever that person is, and that is literally geographically around the country. And we have that presence today with accredited, training, fully capable investigators, both staff and contract.

Mr. MEADOWS. So how long, Mr. Reid, would it take you to get up to speed to match that capacity?

Mr. REID. So our plan is the 36-month plan. We would phrase in incrementally over the 3-year period, so by the end of year 3, our plan would be complete. We would have the capacity and the processes.

Mr. MEADOWS. So how much quicker will you be able to do background checks for DOD, Mr. Reid?

Mr. REID. We would eliminate the reinvestigation, so that's a zero.

Mr. MEADOWS. I'm looking for——

Mr. REID. Let's remove that completely. The goals for the government——

Mr. MEADOWS. You don't remove it, you just move it.

Mr. REID. Well, it just happens contemporaneously.

Mr. MEADOWS. But if Mr. Phalen had the same kind of operation, where it is ongoing, similar to what Mr. Hodgkins is talking about from the technology standpoint, I mean it's a distinction without a difference.

Mr. REID. We see no reason why we cannot hold ourselves to the standards and the goals that we set, which for instance is 80 days for a top secret clearance that is currently taking 350.

Mr. MEADOWS. So your sworn testimony today is that if we allow you to go forward and do this, and we appropriate the dollars to do this, that you can do this at less cost than Mr. Phalen, and make sure that you get it done in 80 days versus 300?

Mr. REID. The cost savings and cost avoidance would be and the reduction of reliance on field investigative work, which is the most resource intensive. Our testing shows us that we can go a very long way towards eliminating, but not completely getting rid of it. The 80-day standard, which has been achieved in government since it was established, it is being frustrated by the lengthy field work. So our rationale is if you get rid of the reliance on the field work, even increased field workers is still more field work. The goal—the DOD objective is to reduce, as much as possible, a 90-plus percent level, the work effort required by a field investigator, and our planning basis is that lowers, that's a cost avoidance issue and there is it no reason to think we cannot operate within the standards that we've already set.

Mr. MEADOWS. Mr.—so let me go ahead bring this to a close, and I guess with a few to-do items.

Mr. Phalen, I would like for you, within a 30-day period, to get back to this committee, what are the three major concerns that you would have, other than just shifting responsibility from OPM, what are the three major concerns that you have in allowing Mr. Reid to go forward with his plan? All right? Can you do that?

Mr. PHALEN. Yes, sir.

Mr. MEADOWS. Mr. Reid, you've had probably more direct questioning today than perhaps you're used to. And call me, you know—we get all kinds of people that come in and testify on a regular basis, and I hear every wonderful story on why it is going to be better, and very seldom do I hear a comment like Mr. Evanina gave me on the excellent work that they are doing and the fact that they are on time and not having roadblocks. And yet, I get to visit Fed-

eral workers in a number of agencies across the spectrum, and we have great Federal workers. So it is not to question anything in terms of your intent. My question is, is sometimes long before what you believe that you can do and actually doing it, there are all kinds of roadblocks that you run into. Some of those many times are financial. And so the last thing I want you to do is to give sworn testimony here today only to find out that all we're doing is shifting it from one agency to another, and that you're going to come in and ask me for more money and more resources to meet that 80-day goal that you have in mind.

So here is my three asks of you: I want you to identify what duplicative services that you would potentially have with OPM if you instituted your plan policy. The other two things is what two things do you not—would you not do as well as OPM under this rollout. Is that something you could provide to this committee in 30 days.

Mr. REID. Yes, sir.

Mr. MEADOWS. And the quicker you can get that to me, because decisions are going to be made on NDAA, even before those—I mean, we're going to conference here soon. And so, Mr. Reid, to be fair to you, I want you to make a compelling case, even if you need to come in and do a briefing with our committee on why it is important to you that things perhaps—because I can tell you your staff has been passing notes back and forth, they are going back and forth doing that, don't ever play poker, but in doing that, they've got all kinds of things that they wish you had said or hadn't said or as we look at that—so as you do that, as your team gets together, I would encourage you to actually come back and brief our committee. Mr. Phalen, I would encourage you the same way. There's going to be some decisions that are made very quickly here on this particular issue. I apologize to both of you that most of the focus has been over here, but sometimes that's the way that things happen when you have this. Again, I appreciate both of you being here as witnesses. The only item—and I see they've passed you a note so are we—when can the ranking member expect those documents?

Mr. REID. So——

Mr. MEADOWS. Within 80 days?

Mr. REID. Friday, sir, Friday.

Mr. MEADOWS. Friday is fine. That would be great. I appreciate it.

I appreciate all of your testimony. Listen, there is nothing more important than getting this right, and getting it right quicker than what we're doing now, Mr. Phalen. I mean, the backlog is, quite frankly, unacceptable. And we wouldn't be having the hearing today if I wasn't hearing it from across the board. That is not to impugn the fine workers at OPM. I understand you didn't create the bureaucracy, but you are here to fix it. And if we can get this fixed, even if it is in a combination of things, I'm all in and all ears. But I thank you all. If there is no further business, the committee stands adjourned.

[Whereupon, at 3:30 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Opening Statement
Ranking Member Gerald E. Connolly
House Committee on Oversight and Government Reform
Subcommittee on Government Operations

Hearing on "Security Clearance Investigation Challenges and Reforms"

October 11, 2017

Thank you, Mr. Chairman, for holding this hearing to examine both the current backlog in federal security clearance investigations and potential reforms to the background investigation process.

Last month, the National Background Investigations Bureau (NBIB) reported a backlog of approximately 700,000 security clearance applications. This backlog and the lengthy wait times for security clearances is unacceptable. It is critical that the NBIB address this problem, and important for Congress to provide it with all of the necessary resources and support to do so.

Since it first began operating on October 1, 2016, the NBIB has been tasked with the challenge of not only improving the federal government's process for conducting background checks, but also bringing down the growing security clearance backlog. In the NBIB's first year in operation, my office received more than three times as many cases as we received in the preceding year where constituents sought our assistance because their background check was seemingly stuck at the NBIB. .

Since its creation, the NBIB has made several enhancements to the security clearance investigation process. For example, it developed a continuous evaluation program for monitoring an employee's or contractor's eligibility to maintain access to classified information or hold a sensitive position.

And earlier this year, the NBIB created a new law enforcement unit to improve the government's ability to gain access to the criminal history records of state and local law enforcement agencies. This is an important change that could eliminate a critical gap in how background checks were previously conducted. That gap has enabled an unknown number of people to gain security clearances they probably should not have received. The importance of gaining access to criminal history records became all too clear on September 16, 2013, when Aaron Alexis, a federal subcontractor with a Secret level clearance, entered the Washington Navy Yard, killed twelve people, and injured four others. During the investigation into that incident, we learned that the background investigation of Mr. Alexis failed to identify his history of gun violence. The local police record of his 2004 firearms arrest had never been provided to federal investigators. Improving the level of communication between local law enforcement agencies and federal background investigators could prevent future tragedies like the one at the Washington Navy Yard.

While the NBIB has made some gains in improving the background investigation process, it has struggled to reduce the heavy backlog of security clearance applications. The current backlog is largely due to termination of the contract that U.S. Investigations Services (USIS) had with the Office of Personnel Management (OPM) to conduct background checks. USIS had previously performed the bulk of background investigations for OPM, but was caught defrauding the federal government on a massive scale: allegedly dumping 665,000 background check cases, indicating to OPM that the background

checks had been complete when the proper reviews had not taken place. OPM had no choice but to terminate its contract with the company. At the time of USIS's termination, it held **60%** of the federal government's investigative capacity for background checks. OPM remains unable to fully replace the significant amount of capacity that was lost with USIS's termination.

Various proposals have been put forward to address the backlog, the most notable of which is a Department of Defense (DOD) plan that would strip the NBIB of its background investigation activities for DOD personnel. Most recently, the Senate has included language in its draft of the National Defense Authorization Act (NDAA) for Fiscal Year 2018 that would adopt DOD's plan.

The DOD plan raises serious concerns, namely that it could potentially increase, rather than decrease, the existing backlog for security clearances. According to the DOD plan, it would take the Department at least three years to assume responsibility from the NBIB for background checks of its personnel. During this three-year transition period, the NBIB would be expected to use its limited resources to help the DOD build the capacity required to perform its own background checks, which may result in additional backlogs at the NBIB. The NBIB has examined DOD's proposal and found it has the potential to "exacerbate the current investigative backlog." OPM has also examined DOD's plan and reached the same conclusion. Outside the federal government, policy organizations, ranging from the Information Technology Industry Council to the Professional Services Council, have reported that DOD's plan would "cause further delays."

Transferring a significant portion of the NBIB's responsibilities back to DOD also risks returning to a process that was previously found to be inefficient. Prior to 2005, DOD was responsible for conducting background investigations of its own personnel. During that time, the Government Accountability Office (GAO) issued a series of reports that raised concerns over the quality and timeliness of those investigations. The most significant of those reports was released in 1999 in which GAO found that "DOD personnel security investigations are incomplete and not conducted in a timely manner." DOD's failure to adequately handle its own security clearance investigations was the primary reason that this responsibility was transferred to OPM in 2005.

Congress needs to seriously examine the best means to reduce the current backlog, but we must do so in a way that balances the need to expedite the process without sacrificing the quality of those investigations. The Navy Yard shooting and high profile national security leaks such as the one carried out by the contractor, Edward Snowden, highlight the need for ensuring that background checks are conducted in a thorough and efficient manner.

I want to thank the witnesses for testifying today. I look forward to hearing from each of you on ways we can strengthen the federal government's capabilities when it comes to security clearance investigations.

Thank you, Mr. Chairman.

Contact: Jennifer Hoffman Werner, Communications Director, (202) 226-5181.

○